Radian Group Inc.

RADIAN

Code of Conduct and Ethics

August 2011

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

Page

TABLE OF CONTENTS
(continued)

Page

Code of Conduct and Ethics

Radian Group Inc.
(and Subsidiaries)

Introduction

Radian Group Inc. has adopted the following Code of Conduct and Ethics (the "**Code**") and has appointed a Chief Compliance Officer to ensure that the standards of professionalism required by Radian Group Inc. are clearly communicated to all of the employees and directors of Radian Group Inc. and its subsidiaries (collectively referred to as the "**Company**"). The Chief Compliance Officer is responsible for establishing a program to enforce compliance with the Code, investigating alleged violations of the Code, and where appropriate, recommending disciplinary actions for violations of the Code.

This Code sets forth general policies of Radian Group Inc., a Delaware corporation; the policies are limited to the extent they conflict with applicable local law (domestic or foreign). It is expected that employees and directors will obey all applicable local laws. Employees and directors are encouraged to contact the Legal department with any questions about whether a proposed course of conduct is proper.

The Company operates in markets which are increasingly competitive and subject to extensive regulation, including by the U.S. Securities and Exchange Commission, various state insurance commissions and a host of other state and federal agencies, as well as foreign laws and regulatory agencies. The Code has been designed to set forth a standard of business conduct that will protect the Company and its employees and directors.

The Code must be adhered to by every person described in the *Applicability* section below. The Code touches on many types of activities and behavior that could expose the Company and its employees, officers and directors to civil and possibly criminal liability. Violations or breaches of the Code may lead to disciplinary action including, where appropriate, immediate dismissal from employment or service without notice. It is the responsibility of every person subject to this Code to report suspected violations of the Code.

Please carefully read the provisions of the Code set forth below. All employees and directors of the Company are, by reason of their continuing employment or service with the Company, deemed bound by the Code, as it may be revised from time to time by the Company. All former employees and directors are bound by the Code to the extent described below.

The Company reserves the right, in its sole discretion, to revise or modify this Code at any time and will provide prompt notice of any changes it has made to this Code. Any waiver of a provision of this Code for an executive officer or director may be made only by the

Company's Board of Directors (or a Board committee) and must be promptly disclosed to shareholders.

Applicability

The Code will be distributed and applies to every director and to every full-time, part-time, temporary or contract employee of the Company, and will be distributed to all new employees as they begin work. Certain provisions of the Code shall also apply to former employees and directors, as described below. As used throughout this Code, the term "**employee**" shall refer to all persons in service with the Company, whether employed on a full-time, part-time, temporary or contract basis. All recipients of the Code must acknowledge receipt of the Code. Compliance with the Code is a condition of continuing employment for every Company employee.

This Code is not to be considered a contract of employment nor does the use of the term "employee" in reference to temporary and contract employees create a contract of employment. All employees of the Company are deemed to be employed on an "at-will" basis and may be discharged with or without cause, at any time, with or without notice, at the sole discretion of management of Radian Group Inc. ("**Management**").

Administration

The Chief Compliance Officer will be the individual responsible for administering, overseeing compliance with, and enforcing the Code; and either the Chief Compliance Officer, Senior Human Resources Executive or General Counsel will make a quarterly report to the Board of Directors of Radian Group Inc. and/or the Compensation and Human Resources Committee or the Audit and Risk Committee, as appropriate, detailing the status of the compliance program.

All determinations related in any way to the interpretation of the Code will be made by the Company in its sole discretion. Employees who have questions regarding the applicability or interpretation of the Code should contact the Chief Compliance Officer, the Senior Human Resources Executive or the General Counsel.

All waivers of any provision of the Code in favor of any executive officer or director of the Company may be made only by the Board of Directors of Radian Group Inc. and shall be promptly disclosed to shareholders in accordance with rules of the U.S. Securities and Exchange Commission.

Incident and Complaint Reporting

1. General

Employees are required to report any potential violations of the Code. Employees may notify the Chief Compliance Officer, Human Resources department, Senior Human Resources Executive, the General Counsel or his or her immediate supervisor (who in

turn is responsible for informing the Chief Compliance Officer of such report) of complaints and potential violations. The Chief Compliance Officer is currently:

Susan Schmidt Pié
Vice President, Associate General Counsel and Chief Compliance Officer
Radian Group Inc.
1601 Market Street
Philadelphia, PA 19103
(215) 231-1574
Susan.Schmidt-Pie@radian.biz

Employees may also leave a message, anonymously if they so choose, in the **Radian Compliance Voice Mail Box,** which can be reached at **800 523.1988 (Ext. 1700).** The individual to whom a complaint or potential violation is made will ensure that it is reported to the Board of Directors (or applicable Board committee), if appropriate. If, after a reasonable amount of time, an employee believes that his or her complaint or report has not been adequately dealt with, he or she may write a letter to the Board of Directors (or the applicable Board committee).

The Company will preserve the confidentiality of all communications regarding potential Code violations. Employees who report conduct which they believe in good faith is or might be a violation of the Code will face no adverse consequences for their report, even if the reported activity does not violate the Code. It is a violation of the Code to suggest that an employee could face repercussions for reporting alleged violations. It is also a violation of the Code for an employee to, in bad faith or with disregard for the truth, report conduct that is not in violation of the Code. It is a violation of this Code to submit a complaint or potential violation knowing it is false.

2. Accounting and Auditing Complaints; Whistleblower Protection

Any employee who is aware of questionable accounting or auditing matters, or of possible financial fraud, should report his or her concerns either: (i) directly to the Chief Executive Officer, President, Chief Financial Officer, General Counsel, Senior Internal Audit Executive, Senior Human Resources Executive, his or her immediate supervisor (who in turn is responsible for informing the Chief Compliance Officer of such report), or Chief Compliance Officer; or (ii) by leaving a message, anonymously if he or she so chooses, on the **Radian Compliance Voice Mail Box (800 523.1988, Ext. 1700).** Any complaints or concerns left in the Radian Compliance Voice Mail Box concerning accounting, internal accounting controls or auditing matters will be reviewed and relayed to the Audit and Risk Committee of Radian Group Inc.'s Board of Directors, as appropriate.

All complaints concerning accounting or auditing matters will be initially investigated by either the General Counsel or Senior Internal Audit Executive, and then relayed to the

Audit and Risk Committee. The General Counsel and Senior Internal Audit Executive may involve the Audit and Risk Committee in an investigation, as they deem appropriate.

Federal whistleblower laws protect employees against adverse employment decisions when employees lawfully provide information to (or otherwise assist in an investigation by) federal law enforcement or regulatory officials, Congress, or any person with supervisory authority over such employees, regarding what the employees reasonably believe to be:

- Possible fraud against the Company's shareholders;
- Possible violations of SEC regulations; or
- Possible violations of federal criminal laws prohibiting mail fraud, bank fraud or fraud by wire, radio or television.

Any employee who believes an adverse employment decision has been made against him or her for any conduct described above is strongly encouraged to notify the Chief Compliance Officer, the Senior Human Resources Executive or the General Counsel, or to leave a message in the **Radian Compliance Voice Mail Box (800 523.1988, Ext. 1700)**, so that the Company has an opportunity to conduct an investigation and take any appropriate remedial action.

3. Harassment

Any employee who believes he or she has been subjected to, or who witnesses, any form of harassment (described below in the Workplace Conduct – Harassment section of this Code) must immediately report the incident(s) to his or her manager or immediate supervisor (each of who in turn are responsible for informing the Chief Compliance Officer of such report), the Chief Compliance Officer or the Senior Human Resources Executive, or leave a message in the **Radian Compliance Voice Mail Box (800 523.1988, Ext. 1700)**. All reports will be handled in a timely, sensitive manner, with the maximum confidentiality possible under the circumstances, as will any investigation and/or disciplinary proceedings.

California employees who believe they have been subjected to sexual harassment may also contact the local office of:

> The California Department of Fair Employment and Housing ("DFEH") at 611 West Sixth Street, Suite 2850, Los Angeles, CA 90017
> Tel. (213) 439-6751; or
>
> The California Fair Employment and Housing Commission ("FEHC") at 455 Golden Gate Ave., Suite 14500, San Francisco, CA 94102

to file a claim within one year of the harassment instead of following the complaint procedures outlined above. The DFEH and/or FEHC serve as neutral fact-finders and will attempt to assist the parties to voluntarily resolve their disputes. If the DFEH or FEHC is unable to obtain voluntary resolution and finds that harassment has occurred, such agencies may award reinstatement or monetary damages.

Business Conduct

1. Integrity

a. Honesty and Good Faith

Each employee and director must act with the utmost integrity, good faith and honesty with regard to the Company and act in the Company's best interests at all times. Each employee and director must deal honestly, fairly and truthfully with the Company, his or her colleagues, and the Company's customers, suppliers, competitors and regulators.

Any failure by an employee or director of the Company to act with integrity and honesty is a violation of the Code and, in circumstances where the employee or director gains a personal benefit from the violation, may constitute fraud. An employee's or director's participation in any way in improper conduct will subject him or her to appropriate disciplinary action up to and including discharge from employment or service, even if that participation resulted from pressure or intimidation from a manager or supervisor. Radian will not tolerate fraudulent activity and any fraud or suspicion of fraud must be immediately reported.

b. Fraud Prevention and Detection

Fraud generally involves an act or omission involving deception or other unethical means that is intended to obtain an unauthorized benefit for either an individual or for the Company. Every employee shares the responsibility to understand and identify fraudulent activity within Radian. A fraudulent act can include, but is not limited to, such things as:

- Embezzlement;
- Forgery or alteration of documents such as contracts, loans, leases, assignments, timekeeping records, production records, analytical results, etc.;
- Forgery or alteration of checks, drafts, promissory notes and securities;
- Any misappropriation of funds, securities, supplies or other Company assets;
- Any irregularity in the handling or reporting of money transactions;

- Theft of materials, furniture, fixtures and equipment or any other Company property;
- Falsification of travel and entertainment expense records;
- Improper financial reporting or recording of fictitious or misleading transactions in the financial records of the Company;
- Expenditures for an improper purpose (i.e., bribery);
- Costs and/or expenses avoided by fraud (i.e., tax evasion); and
- Revenue or assets obtained by fraud (i.e., defrauding customers).

Management has primary responsibility for detecting fraudulent activity within the Company. Each manager should be familiar with the types of fraudulent activity that might occur in his or her area as well as the control activities that are in place to help prevent such activities. Control activities include proper segregation of duties, appropriate authorizations and approvals, verifications, reconciliations, reviews of operating performance, and reasonable steps to secure assets. Information systems play a critical role in internal control and they should be developed and maintained to mitigate fraud risk and assist with the timely detection of fraud. Management should diligently monitor day-to-day operations including control activities and must be alert for any indication that fraudulent activity is or was in existence. Such monitoring by management is in addition to the routine, periodic assessment of internal controls by the Internal Audit function.

Any detection or suspicion of fraudulent activity by management or non-management personnel must be reported immediately using the Incident and Complaint reporting procedures set forth under "Incident and Compliant Reporting" in this Code. Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid incorrect accusations or alerting suspected individuals that an investigation is underway. Accordingly, an employee who suspects or has detected a fraudulent act should not initiate their own investigation or confront the person suspected of such fraudulent act but rather should report the issue immediately.

c. **Full Disclosure**

All employees and directors are expected to cooperate with an investigation conducted by the Company. A failure to cooperate and/or provide full disclosure of information and knowledge of an incident being investigated that may violate any aspect of this Code may itself be a violation of this Code and may result in disciplinary action up to and including discharge from employment or service,

subject to the protections afforded employees under federal whistleblower laws (discussed in the section of this Code entitled *Incident and Complaint Reporting – 2. Accounting and Auditing Complaints; Whistleblower Protection).*

d. **Conflicts of Interest; Corporate Opportunities**

All employees and directors are required to avoid any situation that may involve a conflict between their personal interests and the Company's interests.

Examples of Potential Conflicts:

- Competing with the Company in any of its business activities;
- Owning a financial interest in any entity that does business with or is a competitor of the Company, except for ownership of publicly traded securities that do not exceed 5% of the class of outstanding securities of such entity (also applies to members of the immediate families of employees and directors);
- Providing consulting, managerial or other services to any entity that does business with or is a competitor of the Company; and
- Representing the Company in any transaction in which the employee or his or her close relative has an interest.

The foregoing is not intended to be a complete list of activities that would involve a conflict of interest. Similarly, all employees and directors must refrain from using corporate property, information or position for personal gain.

No employee may serve on the board of directors of more than one publicly traded company other than Radian Group Inc. All employees must report to the General Counsel the name of each company (excluding non-profit organizations) on which they are currently serving, or have been nominated to serve, as a director.

If an employee or director wishes to engage in an activity or enter into a relationship that may involve a conflict of interest for him or her, he or she must first obtain approval from appropriate personnel within the Company by disclosing the potential conflict of interest to the Chief Compliance Officer, the Senior Human Resources Executive or the General Counsel. The Chief Compliance Officer, Senior Human Resources Executive or General Counsel will ensure that the appropriate persons make a determination as to the permissibility of the proposed activity or relationship.

2. Corporate Assets and Accounts

Company employees are expected to utilize corporate assets (such as stationery, office

supplies and equipment, computer equipment, office space and furnishings, and the Company's mail facilities) and corporate accounts (such as messengers, FedEx®, florists, restaurants and hotels) in the normal course of employment or service. Personal use of the Company's mail facilities and of the Company's accounts is prohibited. The misuse or removal without proper authorization from the Company's offices of any of its property or assets is prohibited. This policy also applies to any property designed, created, modified, obtained, purchased, leased or copied by the Company for its own use including, without limitation, files, reference manuals, user guides, reports, forms, policies, computer programs and software, data processing systems and databases.

It is a violation of the Code to make any copies of computer software programs purchased or leased by the Company for its use, except as provided within the particular software licensing agreement. It is also a violation of the Code to: (i) install any software acquired personally on a Company computer without advance approval from the Information Technology department, which may involve checking the software for compatibility and the existence of defects, viruses, etc.; or (ii) use any software acquired personally in violation of such software's licensing agreement.

See the section of this Code entitled Information and Computer Systems Policy for further detail about use of software and personal use of telephones, email and the Internet.

3. Communications with Governmental Agencies and Regulators

Any employee or director of the Company who, in the course of employment or service with the Company, comes into contact with any governmental agency, foreign or domestic (federal, municipal or state), in relation to the Company must take care in making any statements to such agency or its personnel. It is a violation of the Code for an employee or director to deliberately make any false or misleading statements (verbal or written) to any regulatory agency. This policy applies to documents filed with state insurance regulators, such as federal, local and state income or premium tax returns, and the like. Misstatements to governmental officials may expose both the Company and the employee or director involved to civil and/or criminal penalties.

All contacts with governmental agencies involving the Company that are out of the ordinary, or do not occur in the normal course of an employee's or director's regular duties, must be reported immediately to the General Counsel or, in such individual's absence, the Chief Compliance Officer or Senior Human Resources Executive. Reportable contacts include any investigation involving the Company and/or any of its affiliates — even "informal, off-the-record" discussions. Other types of contact that need to be reported immediately include the receipt of a subpoena, written correspondence or telephone or personal contacts. Delays in responding to these types of documents could have adverse effects on the Company's legal position.

This section is not intended to limit any conduct of an employee that is protected by federal whistleblower laws, as described in the section of this Code entitled *Incident and Complaint Reporting – 2. Accounting and Auditing Complaints; Whistleblower Protection.*

4. Bribery, Gratuities and Improper Payments

It is a violation of the Code for any Company employee or director to offer or receive a bribe, kickback, gratuity or other improper payment in order to achieve a desired business result. Providing or receiving a bribe or other improper payment may constitute an unfair business or insurance practice, and therefore may be illegal. Employees and directors who become aware of a request for, or the offering of, any bribe, kickback or other improper payment, whether or not they are personally involved, are required to immediately report such occurrence to the General Counsel or Senior Human Resources Executive.

Employees and directors are not permitted to offer anything of value to a government official in an effort to influence such official or to receive preferential treatment for the Company or any of its affiliates. Any questions regarding the application of this portion of the Code should be directed to the General Counsel.

When contacting representatives of any company (e.g., real estate brokers, vendors, law firms, appraisal companies or customers), no employee or director may extend or receive a gratuity or kickback or other improper payment to influence the placement of business. This prohibition extends to the provision or receipt of free or compensating services for which the recipient would normally incur an expense. Provision or receipt of free services may create an actual conflict of interest and may seem inappropriate, even if completely innocent in nature. Offers of such a gratuity, kickback or free services must be reported to the General Counsel immediately.

In the normal course of conducting routine business activities, many employees entertain (or are entertained by) customers, vendors and others outside of the Company. Any entertainment must be reasonable and not excessive. It is impossible to prescribe a hard-and-fast rule for defining “reasonable” entertainment. A good way to measure the reasonableness of the entertainment is to think how you would explain the entertainment to a regulator or investigator at a later date. If the entertainment in question is of such magnitude that it could be perceived as a key factor in the business decision that was reached, such entertainment is probably unreasonable and should be avoided. Examples of entertainment that would appear to be reasonable would include a single sporting event or dinner. An example of entertainment that would appear to be unreasonable would be the provision of free season tickets for a professional sports team, and the like.

This is an area where a great deal of caution must be exercised by all employees. Employees must consult with the Company’s Legal department any time they have a

question about the propriety of an entertainment expense they are about to incur or for entertainment benefits they have been offered.

5. Proper Accounting Practices

As a regulated entity and a publicly held company, Radian Group Inc. has a duty to its regulators, policyholders and stockholders to maintain its books and records in a manner so that all financial reports and statements accurately reflect the nature of its business affairs. This Code cannot outline each and every accounting standard or practice applicable to the Company's business operations. Management must rely on the integrity, truthfulness and honesty of its employees and directors to meets its financial reporting and disclosure requirements.

All communications with outside auditors must be true and complete. The auditors have a responsibility to determine whether the financial statements of the Company are presented fairly in all material respects. All employees and directors must cooperate fully with the representatives of the outside auditors by responding promptly, accurately and completely to all inquiries received from such representatives. No employee or director may knowingly or recklessly make any false or misleading statement to any outside auditors.

Any employee or director who is aware of misstatements or omissions (intentional or otherwise) in the Company's financial statements or other reports, or questionable or fraudulent accounting practices, should report this information promptly, as described above in paragraph 2 of the section of this Code entitled Incident and Complaint Reporting.

6. Political Activity

All companies are precluded by the laws of the State of Delaware, Commonwealth of Pennsylvania and State of New York (and of many other states and jurisdictions in which the Company has operations) from participating in the political process. No contribution of money, property or services may be provided to any political party or candidate on behalf of the Company. It is a violation of the Code for any employee or director to contribute money or services on behalf of the Company.

Example: Purchasing tickets to political fund raisers and then submitting the receipt to the Company for reimbursement.

Example: Use of Company supplies or equipment to copy campaign materials.

Example: The provision of office space to a candidate or political party at reduced rental rates.

The foregoing is not a complete list of the types of prohibited activities. Engaging in such

activities may expose both the Company and the employee or director to civil and/or criminal liability.

It is also a violation of the Code for any employee or director to, directly or indirectly, require another employee or director to make personal contributions to any political candidate, party or political action committee.

The Company does encourage all employees and directors to become involved in the political process and exercise their rights as citizens. However, employees and directors must take care that their own personal involvement is not attributed to the Company. This section is not intended to dissuade employees and directors from engaging in charitable activities. Employees and directors should not hesitate to contact the General Counsel with questions regarding campaign contributions or other political activity.

Confidentiality

Because Radian Group Inc. is a publicly traded entity, it is imperative that information regarding the Company, its results of operations and future projections and plans be maintained in strict confidence. Improper use or disclosure of confidential information relating to the Company may subject the Company, and its employees, former employees, directors and former directors, to liability, including penalties relating to insider trading. Employees, former employees, directors and former directors should take all reasonable steps to ensure that members of their immediate families and personal households, as well as any persons with respect to whom there is a reasonable expectation of confidentiality, comply with this section of the Code. The term **"Covered Person"** when used in this section of the Code applies to each of the Company's employees, former employees, directors and former directors.

1. Company Confidential Information

Information relating to the operations and results of operations of the Company, past, present and future, its officers, directors, employees, former employees, former directors, business or customers, which has not been publicly disclosed or any information designated by Management as "confidential" shall not be used by any Covered Person except in the course of his or her employment or service with the Company.

Information relating to the competitive plans of the Company including, without limitation, acquisitions/mergers, products under development, marketing plans or promotions, premium or insurance programs, customer lists and any other information relating to the Company's marketing and/or underwriting plans, or relating to the Company's information technology, including, without limitation, technical data, and computer software, is to be kept confidential. No such information shall be disclosed to any person outside the Company, except as required in the normal performance of a Covered Person's service with the Company.

Certain information the Company uses or has access to is protected under applicable federal and state privacy laws, including for example the Gramm¬Leach-Bliley Act (Title V, Subtitle A, 15 U.S.C. § 6801 *et seq.*) and its comprehensive list of privacy restrictions, and is treated as "confidential" by the Company. Such information includes all borrower information that the Company may receive from lenders or from any other sources. No such borrower information shall be disclosed to any person, inside or outside of the Company, except in the normal course of effecting or administering the transaction or project for which the borrower information was received.

All Covered Persons are expected to take the appropriate precautions to safeguard confidential and proprietary information of the Company that is under their control. Covered Persons should contact the Legal Department with any questions regarding the appropriateness of disclosing borrower information.

2. Third-Party Confidential Information

Covered Persons of the Company may, in connection with their prior association with another company or otherwise, possess confidential or proprietary information that belongs to third parties that has not been disclosed to the Company. Such third-party confidential information should not be used in connection with any service for the Company or disclosed to others within the Company, in violation of such confidentiality obligations.

3. Non-Public Information and Trading in Securities

It is a violation of the Code and of the Company's insider trading policy (which appears as the last section of this Code) for any Covered Person to use or disclose material, non-public information that he or she obtains as a result of employment or service with the Company. Such non-public information may pertain to the Company, its customers or any other company.

It is a violation of the Code, and applicable laws, to use non-public, material information in connection with any securities transaction. It makes no difference that the security traded is not one issued by Radian Group Inc. It is also improper to pass on or communicate any non-public, material information to individuals outside the Company who may use such information to purchase or sell securities.

Any person who trades in securities of Radian Group Inc. ("**Company Securities**") while aware of material, non-public information about the Company may be sued in both civil and criminal proceedings for "insider trading." Any person convicted of insider trading may be liable for up to three times the amount of profit gained or loss avoided as a result of any such unlawful sale or purchase transaction. Liability may also arise if such person discloses ("**tips**") material, non-public information to any other person who then trades in the Company Securities. The person receiving the tip (the "**tippee**") can be liable even

when the tippee does not knowingly engage in insider trading. Further, the tipper and tippee may each be subject to liability for the communication of the tip and the resulting transaction, even if the tipper did not profit from the tippee's transaction.

In order to form a basis for liability under federal securities laws, the information which is possessed by a person trading in Company Securities or which is communicated to another person must be both non-public and material. For this purpose, information should be considered non-public for at least two full business days (days on which the New York Stock Exchange is open for trading) after the information has been released to a national wire service.

Information is considered "material" if there is a substantial likelihood that a reasonable investor would consider such information important in making an investment decision.

Examples of the types of information generally deemed to be material include:

- A dividend increase or decrease;
- An earnings estimate or revision of a previously released estimate;
- A significant expansion or curtailment of operations;
- A significant increase or decrease in sales or earnings;
- A purchase or sale of substantial assets;
- Mergers and acquisitions;
- A significant increase or decrease in defaults or claims;
- A tender offer for the Company Securities;
- The development or impending announcement of a significant new product;
- Extraordinary corporate borrowing or a default under a corporate borrowing;
- Major litigation;
- Liquidity issues; and
- Extraordinary Management developments.

This list is not intended to be exhaustive, and other corporate developments may be material depending upon the circumstances at that time.

Any questions regarding confidential information and trading in securities should be

directed to the General Counsel or, in his absence, to the Chief Financial Officer. The Company's Policy Regarding Securities Trading appears as the last section of this Code of Conduct and Ethics.

4. Communications with the Public

Federal securities laws govern the timing and nature of the Company's disclosure of material information to the public. Violation of these laws could result in substantial liability for Covered Persons, the Company and Management. The Senior Investor Relations Executive and Senior Marketing Services Executive are responsible for the Company's communications with the public and arrange for the public release of Radian Group Inc.'s quarterly and annual financial results. The Company's Disclosure Committee oversees the general disclosure process, and helps ensure the accuracy of information, for all public disclosures of Company information, pursuant to the Company's written Disclosure Controls and Procedures.

Covered Persons who receive general inquiries relating to the Company from outside sources must refer such inquiries to the Senior Investor Relations Executive or Senior Marketing Services Executive, or in those individuals' absence, the Chief Executive Officer, President, Chief Financial Officer or General Counsel. Such requests may come from reporters, government officials or others. Requests for information from securities analysts, stockholders or investors should be referred directly to the Chief Financial Officer. These restrictions, however, are not intended to prohibit a Covered Person from lawfully providing information to the authorities as part of an investigation of corporate conduct where the Covered Person reasonably believes such conduct to be possible fraud against the shareholders or a possible violation of Securities and Exchange Commission regulations or certain other federal fraud statutes, as more fully described above in paragraph 2 of the Incident and Complaint Reporting section of this Code.

Accidental disclosure of information about the Company can be as harmful as a deliberate leak. An accidental disclosure could occur, for example, if sensitive information is discussed in public places, confidential documents are left in public areas, or if highly confidential corporate information is the subject of family discussions. Premature disclosure of the Company's financial results could result in severe and unfavorable consequences for the Company and the individual disclosing the information.

It is the obligation of every employee and director of the Company to take prudent and reasonably necessary steps to preserve the confidentiality of the Company's business information. In this regard, see also a description of confidentiality safeguards in this Code under *Information and Computer Systems Policy —Confidential and Proprietary Information*.

Failure to comply with the foregoing provisions of the Code may violate applicable

federal and state statutes and subject the Covered Person and the Company to civil and criminal liability.

Workplace Conduct

1. Equal Employment Opportunity

The Company recognizes the freedom, rights and dignity to which each individual employee and applicant for employment is entitled. It is a violation of the Code and applicable laws to make employment decisions based upon an employee's or applicant's race, creed, color, age, gender, marital status, national origin, ethnic heritage, religion, sexual orientation, or veteran status. It is also a violation of the Code and applicable laws to retaliate against an employee or applicant for making any complaint about, or for opposing, any allegedly discriminatory conduct, when the individual making the complaint or opposing the conduct does so on a good-faith belief that he or she is complaining about or opposing unlawful practices and such individual expresses his or her complaints or opposition in a reasonable manner. Any employee having doubts about whether any complaints or expressions of opposition are protected should assume that they are protected, unless the employee is informed by the Human Resources department, the Legal department or the Chief Compliance Officer that such conduct is not protected.

The Company is committed to providing equal employment opportunities. Each department manager is responsible to ensure that this policy is followed.

All employees are encouraged to follow the enforcement and complaint procedures described above in the Incident and Complaint Reporting section of this Code.

2. Nepotism and other Personal Relationships

No two employees who are in a personal relationship with each other can be in a direct or indirect reporting relationship. Furthermore, individuals in personal relationships may not work in the same department or in positions that may compromise internal audit separation of responsibilities objectives. No exceptions to this policy will be permitted without the advance review and approval of the Human Resources department and the Chief Executive Officer. For purposes of this section, a "personal relationship" includes a spouse, parent, step parent, parent-in-law, child, step child, sibling, sibling-in-law, aunt, uncle, grandparent, grandchild, legal guardian, niece, nephew, fiancé/partner of any gender, or a person with whom one has a romantic relationship. This policy is intended to ensure fair and equitable treatment of all employees and to avoid potential conflicts of interest, criticism and employee morale problems. Employees are encouraged to seek guidance from the Human Resources department about potential conflicts caused by these types of relationships.

3. Harassment

The Company is committed to maintaining a work environment that is free of any form of employee harassment based on gender, race, creed, color, religion, national origin, ethnic heritage, age, marital status, sexual orientation, veteran status or any other unlawful basis.

Harassment is unacceptable in the Company's offices or in other work-related settings such as business trips, business meals and business-related social events. Harassment can be perpetrated by a fellow employee, a supervisor or a non-employee who conducts business with the Company (such as a vendor or customer).

Experience has shown that harassment can occur not only when one individual deliberately intends to harass or "pick on" another person, but also when individuals believe they are "just kidding," or when they make jokes or commit pranks that they think are funny but do not realize are offensive to others. Employees overhearing such statements or witnessing such conduct may be initially reluctant to "make an issue" out of such behavior, and thus the offending party perhaps might believe incorrectly that no one was offended by his/her conduct. These problems can be avoided if employees use discretion, good taste, common sense and basic courtesy at all times in and outside the workplace.

Thus, Company policy strictly prohibits any kind of banter or jokes in or outside the workplace that are of a racial, ethnic, sexual or religious nature, or that pertain to such subjects as disabilities, sexual orientation, or a person's personal characteristics or background. Claiming that other employees were participating in such conduct or that no one complained or seemed offended at the time will not be an acceptable defense under this policy.

All officers, managers and supervisors are responsible for implementation of the Company's harassment policy and for ensuring that all employees they supervise have knowledge of and understand the policy. The Company requires the reporting of all incidents of harassment — employees should follow the complaint procedures described above in *the Incident and Complaint Reporting* section of this Code. The initiation of a complaint, in good faith, shall not, under any circumstances, be grounds for discipline. It is a violation of the Code and applicable law for an individual to be disciplined or otherwise disadvantaged as a result of the good-faith resort to the complaint procedure.

Harassment can take any form. Some examples are discussed below.

a. Verbal or Visual Harassment

This includes derogatory or vulgar remarks about a person's race, creed, color, age, gender, marital status, national origin, religion, ethnic heritage, sexual

orientation, veteran status, physical or mental disability or physical appearance; threats of physical harm (see also the *Violence in the Workplace Policy* in this Code of Conduct and Ethics); and production and/or distribution of graphic material having such effect.

b. **Physical Harassment**

This includes hitting, pushing, aggressive physical conduct or threats to take such action (see also the Violence in the Workplace Policy in this Code of Conduct and Ethics).

c. **Sexual Harassment**

Sexual harassment in any form will not be tolerated. It does not matter if the victim is male or female. Sexual harassment is a violation of the Code and is also a violation of Title VII of the Civil Rights Act of 1964, as well as the laws of the Commonwealth of Pennsylvania, the State of New York and many other states and countries in which the Company does business. Any employee who feels that he or she may be a victim of, or is aware of, a harassment situation should contact the Human Resources department, Chief Compliance Officer, Senior Human Resources Executive or General Counsel.

Prohibited Conduct

Sexual harassment refers to unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature when: (1) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment or service; (2) submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting such individual; or (3) such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile or offensive working environment. Any conduct of the type described above is a violation of the Code, regardless of whether or not submission to such conduct is made a condition of employment or service.

Depending on the circumstances, sexual harassment may include, but is not limited to, the following types of conduct: unwanted sexual advances; subtle or overt pressure for sexual favors; sexual jokes, flirtations, innuendos, advances or propositions; graphic or suggestive commentary about an individual's body, appearance, sexual prowess or sexual deficiencies; leering, whistling or unwelcome physical contact; suggestive, insulting or obscene comments or gestures; unwelcome gifts; unwelcome questions about a person's sex life, dating

relationships or sexual preferences; and the display or distribution in the workplace of sexually suggestive or demeaning objects, pictures, articles or other items.

The Company will not accept as an excuse to a complaint of sexual harassment that an employee was "only joking" or "didn't think the other employee would object."

d. **Hostile Work Environment**

Conduct that has the purpose or effect of unreasonably interfering with an individual's work performance or creates an intimidating, hostile or offensive working environment is a violation of this Code. Any employee who feels that he or she may be a victim of, or is aware of, a hostile work environment situation should contact the Human Resources department, Chief Compliance Officer, Senior Human Resources Executive or General Counsel.

4. Employee Safety

The Company is committed to providing employees with a safe workplace.

a. **Violence in the Workplace**

Any type of violent behavior including any threats, threatening language or any other acts of aggression or violence made against an employee, client, visitor or anyone by anyone while on Company premises or conducting Company business is absolutely prohibited. Threats of violence include throwing objects, menacing gestures, damaging property, flashing weapons, stalking or verbal or physical abuse. Possession of any firearms, knives, explosives or other weapons or dangerous materials is absolutely prohibited.

Employees who witness or are the victims of violent behavior or threats of violence must report the information to their immediate manager, the Human Resources department, the Chief Compliance Officer, the Senior Human Resources Executive or the General Counsel immediately.

Employees who are aware of a potential risk of violence at the Company from an individual not related to the Company (such as an ex-spouse, partner, boyfriend or girlfriend or any other person) are encouraged to report that information to their immediate manager or to Human Resources. Any employee that has obtained a protective or restraining order that lists the Company's locations as protected areas must provide a copy of the order to the Senior Human Resources Executive or General Counsel.

b. **Cell Phone Usage**

The need for a cell phone is crucial in the productive day-to-day activities of certain employees of the Company. Although the Company acknowledges the need to have the cell phone accessible to such employees at all times during the workday, the safety of those employees and any bystanders must take a priority.

The Company discourages employees and directors from using a cell phone while driving an automobile. Employees and directors must adhere to all state and local laws in this regard. If an employee or director chooses to use a cell phone while driving in an area that allows such use, the Company recommends using a hands-free device to mitigate safety concerns, and finding a proper parking space prior to using the cell phone. Parking on the side of a road is not acceptable except in the case of genuine emergencies such as an accident or automobile breakdown. As a reminder, proper use of cell phones is only one aspect of safe driving. The driver should operate the automobile in a safe manner at all times.

5. Substance Abuse

The Company is committed to providing a safe workplace and to establishing policies that promote and encourage high standards of employee health and safety. It is impossible to maintain a safe, healthy working environment if any employee allows the use of alcohol or drugs to interfere with the performance of his or her job or the operations of the Company. The use, sale, purchase, possession or transportation of illegal drugs on Company property, during working hours, or while on Company business is expressly forbidden. The proper use of drugs or medicine prescribed by a licensed physician for an individual employee is permitted but must not affect work performance. Similarly, employees are expected to be responsible in their use of alcohol, and any excessive use of alcohol is also expressly prohibited. A very moderate use of alcohol may be customarily appropriate when entertaining during a Company-sponsored event or when entertaining Company customers, even on Company premises. At these times, the Company expects all behavior to remain within a prudent and conservative standard of professional, mature behavior.

Employees with drug, alcohol and/or personal problems are encouraged to seek early assistance. The Company offers all employees confidential access to an outside Employee Assistance Program. No employee with a drug or alcohol abuse problem will have his or her employment or service with the Company jeopardized because of a request for help. An employee with a drug and/or alcohol problem who refuses to report

to an approved counseling or rehabilitation program or who leaves a treatment program before being released may be subject to immediate discharge from employment or service.

The Company reserves the right to require an employee or director to undergo a drug or alcohol test when the Company reasonably suspects that the employee is using drugs or alcohol in violation of the Code.

Officers, managers, supervisors and employees who may suspect a violation of the Company's substance abuse policy are expected to inform the Human Resources department or their managers in a timely fashion. Any violation of this substance abuse policy should be reported to the Chief Compliance Officer, Senior Human Resources Executive or Human Resources department.

6. Antitrust

The Company is committed to vigorous competition in the marketplace. Conduct or behavior aimed at limiting competition is inconsistent with this commitment and may violate state and federal antitrust statutes.

Such violations may result in serious consequences. For instance, conduct violating the antitrust laws may result in criminal penalties. A corporation may be fined up to 10 million dollars if convicted. Individuals participating in the conduct may be fined up to $350,000 or imprisoned for up to three years, or both. In addition, antitrust violations may result in costly private lawsuits and civil damages.

This Code requires full and complete compliance with all antitrust laws. The following sections outline some of the major aspects of the antitrust laws. This brief overview cannot address the complexities of all of the antitrust regulations. Employees and directors should refer any questions regarding the application of these policies to the General Counsel.

a. Price Fixing

It is a criminal violation of the antitrust laws to enter into any agreement or understanding, no matter how informal, with a competitor concerning the price of a product or service. This prohibition applies to any agreement or understanding to increase, decrease or stabilize prices, agreements or understandings concerning any component of a price, and any agreements or understandings concerning the terms or conditions of a sale of a product. The simple exchange of price-related information between competitors, such as costs, profit margins, internal returns on equity, premium increases, commission structures and loss reserves can be used to

infer an agreement or understanding to fix prices. Employees and directors of the Company are prohibited from entering into any agreements, understandings or discussions with competitors to fix prices.

b. **Agreements to Divide Markets/Customers**

It is a criminal violation of the antitrust laws for competitors to agree to allocate markets, business opportunities, territories or customers among themselves. The Company cannot agree with a competitor to refuse to bid for particular types of business or otherwise refrain from competing for certain customers or classes of customers. Such market allocation agreements or understandings are prosecuted vigorously by the federal government and other regulatory bodies under applicable local law. Involvement in such activities exposes the Company to significant potential liability and may also expose individuals involved to serious personal liability. Employees and directors of the Company are prohibited from entering into any agreements, understandings or discussions with competitors concerning insurance markets, customers and territories.

c. **Group Boycotts/Refusals to Deal**

Group boycotts, or concerted refusals to deal, may be illegal. Accordingly, while the Company has the right to select those companies and individuals with whom it will and will not conduct business, the Company cannot agree with any of its competitors, customers or others not to do business with another person or entity. No director or employee of the Company may agree, or even participate in discussions, with a competitor, customer or other individual or entity concerning the status of any of the Company's business relationships. For example, the Company can refuse to accept insurance applications from a particular broker — the Company cannot recommend or even discuss with a competitor that it do the same. Similarly, the Company can refuse to accept insurance applications from a broker or other mortgage originator on the basis of a history of poorly originated loans — the Company cannot advise other insurers or investors not to deal with such broker or originator, nor can the Company refuse to do business with an individual or entity at the request of another originator or broker.

d. **Monopolization and Market Power**

It is illegal for a company to control prices within a particular market or to exclude others from that market through that company's size and market power. Market power alone, however, is not illegal. An illegal monopoly is one that is obtained or maintained through an abuse of power. This Code prohibits the use of competitive tactics that could be construed as being designed to exclude or destroy competition in any market. Thus, it is contrary to this Code to say or do anything designed to harm a competitor except through the Company's superior

product and service. Questions about the legality of any particular competitive tactic should be directed to the General Counsel.

e. **Tying or Reciprocity**

"Tying" and "Reciprocity" are the mirror images of each other. Tying is the refusal to sell one product or service unless the customer buys another product or service. Reciprocity is the refusal of a purchaser to buy a product or service unless the seller agrees to buy some other product from the purchaser. Such agreements may be illegal if they allow a company to use its power in one market to obtain an unfair advantage in another market. Any tying or reciprocal agreement raises potential antitrust concerns and must be reviewed in advance by the General Counsel.

f. **Other Agreements Among Competitors**

Not all cooperative activity between competitors automatically violates the antitrust laws. Some cooperative activity may increase or be consistent with competition. Such cooperative activity is permitted by the antitrust laws. For example, certain types of conduct such as participation in state-regulated or -sanctioned rating bureaus or risk pools or syndicate arrangements may be exempted from the antitrust laws because they fall under state regulation. Other types of cooperative conduct such as the establishment of non-price-related industry standards are not automatically illegal and are subject to a case-by-case review to determine whether they increase or decrease competition. Because of the risk that cooperative activity may be illegal, however, directors and employees must consult with the General Counsel prior to taking any steps to participate in a cooperative arrangement with competitors.

g. **Trade and Professional Associations**

Trade associations and professional groups provide opportunities for valuable business, social and educational activities for their members. These activities are legal and permissible under the various antitrust statutes. However, because trade association meetings bring together competitors, they present opportunities for activities that may not be permissible. Permissible trade association participation may include working with customers and competitors on matters such as lobbying and legislative issues that affect the lending and/or housing industry. An example would be a joint effort to effect needed changes in legislation authorizing a state housing finance agency. Discussions relating to issues and information of a sensitive, competitive nature must be avoided. Any mention of premiums, costs, marketing strategies, customers, territories and any other issues with an impact on competition between the Company and others is prohibited.

If, in connection with a trade or professional association meeting, any discussion begins that deals with competitively sensitive issues, representatives of the Company in attendance should attempt to stop the discussion immediately. If the discussion continues, the Company's representatives must leave the meeting immediately. Prior to leaving, an effort should be made to have an entry made into the formal minutes (if any) of the meeting detailing the reason that the Company's representatives chose to leave. A detailed written report on the incident should be prepared and forwarded to the General Counsel.

h. **Agreements Regarding Salary Levels or Hiring Practices**

The Company may not agree with other employers to limit pay increases to a given amount or percentage. Nor may the Company agree with another employer to refrain from hiring each other's employees or in any other way not to compete with respect to hiring. Discussions or arrangements with other employers regarding salary levels or hiring practices, from which agreements concerning compensation and hiring practices might be inferred, are prohibited. Any violation of this section of the Code must be reported to the Director of Human Resources, the General Counsel or the Chief Compliance Officer.

i. **Collection of Competitive Information**

The Company is entitled to collect information on premiums and other topics concerning the competitive practices of its competitors. Such market information enables the Company to offer services and products in the marketplace that are competitively priced and better than those of the competition. However, an exchange of information between competitors may indicate the existence of an antitrust conspiracy. Accordingly, no director or employee of the Company should obtain policy forms, premium schedules or rate cards or any other competitive information (unless the information is publicly available) directly from a competitor. Similarly, no Company director or employee should provide competitive information to a competitor. It is permissible to obtain competitive information from third parties such as customers, brokers, etc. It is also acceptable to obtain the information from public sources such as state rate and forms filings with insurance departments. Whenever a director or employee obtains a competitor's rates or policy forms or other competitive information, the source of the information should be documented.

Information and Computer Systems Policy

1. Introduction

a. Information and Computer Systems Covered by the Policy

The Policy applies to and governs the use of the information and computer systems ("Systems") of the Company, as these Systems may be modified from time to time. For the purpose of the Policy, the covered Systems include but are not limited to the following:

- Electronic mail (email) access and usage;
- Voice mail access and usage;
- Internet access and usage, including the World Wide Web and sites accessed using browser programs;
- Mainframes, midrange and file servers;
- Computer networks;
- Employee workstations;
- Desktop, laptop or notebook computers, palm-top computers, personal data organizers or personal computers, irrespective of where used;
- Electronic media, including, but not limited to, floppy disks, compact disks ("CDs"), digital video disks ("DVDs") or magnetic tapes;
- Modem, printers or other peripheral equipment;
- Electronic files;
- Program applications;
- Software, either owned or licensed by the Company;
- Files, records, data, messages and information on the System or its components;
- All other elements of the Company's computer facilities and networks; and/or
- Physical facilities which house the Company's systems.

b. **Questions About the Policy**

All questions an employee or director may have about the Policy should be directed to his or her immediate manager or department head, or to the Chief Information Officer or the General Counsel (or their respective designees).

c. **Employees' and Directors' Responsibilities and Acceptance of the Terms of the Policy**

It is each employee's and director's responsibility to use the Company's Systems only as authorized and in a professional and responsible manner.

2. Ownership of Systems and Employee Work Product

All elements of the Company's Systems are owned by or licensed to the Company. All Systems, including hardware and software, are the property of the Company. Records, files, data, messages, information and electronic communications contained in these Systems are also the property of the Company.

No employee or director has any ownership interest or rights, to any degree, in any of the Company's Systems, or any of the records, files, data, messages, intellectual property or information contained in the Systems. Any Systems created by Company employees during the performance of their duties as employees are property of the Company, and employees cannot take any such Systems with them when their employment or service with the Company ceases. More specifically:

- All confidential information and all other discoveries, inventions, processes, methods and improvements which were conceived, developed or otherwise made by a Company employee alone or with others at any time during the period of the employee's employment or service with the Company and which in any way relate to the Company's present or future business or products, whether or not patentable or subject to copyright protection and whether or not reduced to tangible form or reduced to practice ("Developments"), shall be the sole property of the Company.

- Every employee: (1) agrees to, and hereby does, assign to the Company all of the employee's right, title and interest throughout the world in and to all Developments; (2) agrees that all Developments shall constitute works made for hire under the copyright laws of the United States; (3) hereby assigns to the Company all copyrights, patents and other proprietary rights that the employee may have in all Developments; (4) hereby waives, to the fullest extent permitted by law, all of his or her moral rights in the Developments; and (5) hereby grants the Company a nonexclusive, royalty-free, irrevocable, perpetual, worldwide license to make, have made, modify, use and sell any prior invention,

development, improvement, trade secret or original work of authorship that the employee may have made prior to his or her employment or service with the Company, which belongs to the employee and which he or she has incorporated into a Company product, process or machine in the course of his or her employment or service with the Company.

- Every employee must make and maintain adequate and current written records of all Developments, and must disclose all Developments fully and in writing to the Company promptly after development of the same, and at any time upon request.

3. Modification of Systems

a. **Modification of System Hardware is Prohibited**

Employees and directors are prohibited from making, in any manner, any hardware modifications to Company Systems or equipment, or to use hardware brought in from outside the Company, without the prior written approval of the Chief Information Officer, or his or her designee.

b. **Modification of System Software is Prohibited**

The Company provides training and support on applications and software as determined by the Information Technology ("IT") department. The IT department may make modifications to this list at any time.

Employees and directors are prohibited from installing any software whatsoever onto the network or other Systems without the prior written approval of the Chief Information Officer or his or her designee.

Employees and directors are prohibited from disabling Company-installed software.

c. **Use of Virus-Checking Software**

Company-approved virus-checking software is installed and must be kept operational on Company Systems. It is a violation of this Policy to disable Company-approved virus-checking software without the prior written approval of the Chief Information Officer or his or her designee.

4. Use of Company Systems

a. **Systems are for Company Business**

The Company's Systems are provided to employees and directors at the Company's expense to assist employees and directors in carrying out the

Company's business. The Company's Systems permit employees and directors to perform their jobs, share files and communicate with each other internally and with selected outside individuals and companies that the Company, in its sole discretion, decides should be accessible for communication or connected to the system.

The Company's Systems are to be accessed and/or used only for Company-related business purposes, except that occasional personal use is permitted as long as such use does not interfere with or harm Company usage or activities.

Use of Company Systems (including its networks or access to the Internet) to engage in commercial activities for an employee's or director's own benefit, or for the benefit of anyone other than the Company, is expressly prohibited.

b. **Prohibited Actions**

It is prohibited for any employee or director to:

- Use any Company System to violate any Company policy, or any applicable law or regulation;
- Damage or disable any Company System or System component;
- Use any Company System to carry out any non-Company commercial business;
- Without proper authorization, remove or destroy records, files, data, information, messages or communications on Company Systems;
- Without proper authorization, access, review, copy, forward, distribute or use, or attempt to access, review, copy, forward, distribute or use, any records, files, data or other information in Company Systems;
- Access, attempt to access, use or disseminate any password or security clearance of another user, or one not assigned to the user; or
- Breach or attempt to breach System security measures.

It is also prohibited for any employee or director to engage in the access or use of any Company System (including, but not limited to, email or voice mail systems) to create, reference, send, transmit, distribute, print, publish, store or download any records, files, data, information, messages or communications which, in any manner:

- Violates Company policies;

- Harasses, threatens, abuses, or is intended to embarrass, denigrate or cause distress or discomfort to another individual or entity;
- References or contains unlawful, harmful, defamatory, offensive, discriminatory, derogatory, vulgar, obscene, hateful, pornographic or otherwise objectionable material of any kind;
- Could constitute or encourage conduct that would be considered a criminal offense, or otherwise a violation of any law, obligation or regulation having the force of law;
- Contains non-authorized personal information;
- Impersonates or purports to be from someone other than the employee or director;
- Allows non-authorized individuals or parties to access Company confidential or proprietary information;
- Violates a person's right to privacy;
- Violates the patent, copyright or trademark rights of other parties;
- Uses or discloses the confidential or proprietary information of other parties that the employee or director does not have authorization to disclose;
- Contains chain letters of any kind; or
- Denigrates or is intended to denigrate the Company or its stockholders, directors, officers, employees, agents, businesses, products or customers.

5. Company Access to and Monitoring of Systems

a. Company Access and Monitoring

There are many reasons why the Company may need to access and/or monitor the Company's Systems, including, but not limited to, employee email, voice mail, Internet access or transmissions, computer files, the network or other Company property or Systems. Some of these reasons include the need to continue to conduct ongoing business, to access information or data when an employee is unavailable; to respond to requests by outside auditors; to respond to or gather information relating to Company disputes or litigation; to maintain quality control; to conduct training activities; to monitor task or job performance or to investigate employee conduct. The Company reserves the right, for any of the

above-listed reasons or for no reason, and without notice, to access or monitor the Company's Systems or employee and director usage or communications.

While occasional, personal use of Company Systems (including telephones) is permitted, Company Systems, their contents and System usage are subject to inspection, examination and/or monitoring by authorized Company representatives at any time, without notice to employees or directors.

Additionally, the Company reserves the right, without notice to employees or directors, to access, review, copy, modify or delete any information transmitted through or stored on its Systems or network, including email communications, voice mail communications and word processing and data files. The Company further reserves the right to disclose any such information to any party (inside or outside the Company) that the Company, in its sole discretion, deems appropriate.

Any files, data, information or messages containing the personal information of an employee or director as a result of the employee or director making occasional use of a computer, telephone or other System component for personal purposes, including transmission of personal email or voice mail messages, will be treated no differently than other files. Accordingly, employees and directors have no expectation of privacy or ownership with the use of the Systems, networks, email, voice mail or other Systems, or with the transmission, receipt or storage of information contained within them.

Employees and directors should not use the Company's Systems, including, but not limited to, voice mail or email, to send, receive or store any personal information that they wish to keep private.

Employees and directors should be aware that the System and System components may automatically record and store information relating to employee or director usage of Company Systems.

Employees and directors must have proper authorization from the Chief Compliance Officer, Human Resources department, Senior Human Resources Executive or Legal department to access any employee's email or voice mail account. Failure to obtain such approval will result in disciplinary action against the person accessing the account, up to and including immediate discharge from employment or service.

b. **Deletion of Records or Files**

Employees and directors should be aware that System hardware, software and programs record a variety of information and data, and that even when an employee or director deletes or erases a record, file or electronic communication,

in whole or in part, such deleted material may still be retrievable at a later time.

Employees and directors should consider the Company's computer facilities and network a shared-file system under which files sent, received or stored anywhere in the system will be available for review and use by any authorized representative of the Company. The same is true of records, files and electronic communications sent out of the office to third parties. Moreover, the recipient or reviewer of files often is able to retrieve "hidden" information and at least some of the material that the creator or sender of the file has "deleted."

6. Security and Passwords

a. System Security

Security of the Systems is a key priority of the Company. Employees and directors are prohibited from breaching, or attempting to breach, System security measures.

If an employee or director believes he or she has discovered a security problem on any of the Systems, he or she should notify his or her immediate manager and the Chief Information Officer or General Counsel immediately. The employee or director should not communicate or demonstrate the security problem to other users of the System.

b. Passwords

Employees and directors are prohibited from using any password other than their own, and must protect against unauthorized access to files on which they are working (note, however, that individual passwords do not prevent authorized Company representatives from accessing those files).

Employees and directors may not disclose personal or System passwords to anyone other than Company representatives specifically authorized to receive them. Employees and directors should take reasonable measures to keep their passwords secure. If an employee or director has reason to believe that someone else is aware of the password of that employee or director or another individual, they should contact the IT department. Every employee and director is responsible for any information transmitted through the network under the employee's or director's password. System logs exist on the servers that identify which person signs into which computer.

Employees and directors are prohibited from using another individual's password without express written permission of the IT department, or from attempting to log on to the network as a system administrator.

7. Confidential and Proprietary Information

Unless special precautions are taken, communications and messages on the Internet, email and voice mail systems pose a risk of interception by or distribution to non-authorized recipients. To the extent a former employee or former director has confidential or proprietary information regarding the Company, such former employee or former director may not use or transmit such information other than as described in the Code.

a. Internet

Employees and directors must assume that the Internet and similar services are not secure — that is, unless special encryption programs are utilized, messages may not be private and may be accessed by unauthorized persons. The IT department can assist if encryption is required. All employees must consult with their manager, and directors must consult with Management, before sending or transmitting unencrypted confidential or proprietary Company information over the Internet.

b. Email and Voice Mail

Most email messages are transmitted over the Internet. Additionally, most voice mail systems are susceptible to interception. The IT department can assist if encryption is required. All employees must consult with their manager, and all directors must consult with Management, before using voice mail or email to send or transmit unencrypted confidential or proprietary Company information.

Additionally, it is important to recognize that voice mail and email systems make it easy for someone to take a message or other information and preserve, copy or distribute that message to multiple parties, in some cases far beyond what the sender of the message intended. Accordingly, employees and directors should carefully screen any email or voice mail communication for content before transmission. Further, employees and directors should use care in addressing email or voice mail messages to make sure that messages are not inadvertently transmitted to an unauthorized person. In particular, employees and directors should exercise care when using distribution lists to make sure that all addressees are appropriate recipients of the information. Individuals using lists should take measures to ensure that the lists are current.

c. Other Safeguards for Confidential or Proprietary Information

Confidential or proprietary information should never be transmitted or forwarded to outside individuals or companies not authorized to receive that information, or to other persons inside the Company who do not need to know that information.

Confidential or proprietary information should not be displayed on a computer screen when a computer is unattended. All personal computers or similar System components should be shut down at the end of each business day.

Employees and directors should not leave portable electronic media or backup tapes that contain confidential or proprietary information open to access by third parties. Such media should be kept locked in drawers or file cabinets, or otherwise secured. Former employees and former directors must return all portable electronic media or back up tapes to the Company upon termination of employment or service.

If employees or directors transmit any information to third parties using portable electronic media, they should be sure that the item (floppy disk, CD, etc.) has not previously been used. Otherwise, it may contain confidential information that the employee or director did not intend to transmit. That information may be retrievable even through an effort was made to "delete" it.

Employees and directors should be aware that many electronic files contain "hidden" data such as author annotations, information concerning the creation and editing of the document, and recent changes to the document. Consult the IT department before circulating any electronic file if you are concerned about the dissemination of such data.

8. Attorney-Client Privileged Communications

Some of the email messages or memoranda sent to employees or directors or stored on the Company's Systems may constitute confidential, privileged communications between the Company and its attorneys, or be protected by another legal privilege. Never forward messages or other communications that are marked as subject to attorney-client privilege or attorney work product privilege to any other individual without first consulting with the Company's Legal department.

Privileged information should not be displayed on a computer screen when a computer is unattended.

Attorney-client and work product privileged communications should not be transmitted over the Internet or any similar non-secure service without specific approval of the Company's Legal department.

9. Software, Copyright and Use Restrictions

The Company licenses the use of computer software from a variety of outside companies. In such cases, the Company may be precluded from copying or distributing such

software, from installing it on certain machines, or from disclosing it to third parties. It is prohibited for any employee or director to take any action in violation of applicable license agreements.

Use of the Company's Systems to copy and/or transmit any software program, document or other information protected by the copyright laws is prohibited by U.S. federal law. Use of the Company's Systems for this purpose may subject employees, directors and the Company to civil and criminal penalties.

Employees and directors should never copy software programs of any kind, including programs on the Company's computer network, without authorization from the IT or Legal departments.

Employees should not accept copies of any software programs from other employees, or persons outside the Company, or download programs from the Internet without advance approval from the IT department. This includes, without limitation, screen savers, as well as any type of software used in an employee's daily work.

10. Laptop or Notebook Computers

Extra precautions should be exercised when taking confidential or proprietary Company or other information out of the office in a laptop or notebook computer. Employees and directors should never leave a laptop or notebook computer that contains such information unattended in public areas.

11. Additional Guidance

In addition to the requirements of the section of this Information and Computer Systems Policy entitled *Use of Company Systems*, while using Company email, voice mail and Internet access, employees and directors should be further guided by the following:

a. Email, Voice Mail and Internet Usage

It is not advisable to send "joking" or humorous messages. Intended sarcasm can be lost without facial expressions or voice intonations, and a later reading of the message can result in a distorted communication unintended by the original sender. Jokes concerning personal characteristics, lifestyle, gender, race, religion, national origin, disability or sexual preference are unnecessary and strongly discouraged.

Use discretion. Despite precautions, messages may be forwarded (perhaps accidentally) or viewed over a recipient's shoulder.

Unless specifically authorized by the Chief Information Officer or Management

(or their respective designees), employees and directors are prohibited from initiating or sending Company-wide or division-wide broadcast messages on Company email or voice mail systems.

Unless specifically authorized by the Company manager in charge of an office location, or his or her designee, employees and directors are prohibited from initiating or sending location-wide broadcast messages on Company email or voice mail systems.

b. **Internet Usage**

Only those employees or directors who are expressly authorized by the Company to speak to the media or the public may use the Company's Systems to speak to, send messages or other information to, or write in the name of the Company to any media location or newsgroup.

In any Internet communication using Company Systems, the employee or director must at all times adhere to all Company policies, and refrain from expressing personal opinions or unauthorized political, religious or other advocacy. He or she also must refrain from unauthorized endorsement or appearance of endorsement of any non-Company commercial product or service. These requirements apply even when the employee or director believes that he or she has not been identified as a Company employee, agent or director.

Unless expressly authorized by the Company, employees and directors are prohibited from using Company Systems to discuss the Company or matters related to the Company in chat rooms, message boards or newsgroups, even if they are not identified at that time as Company representatives. Employees and directors are further prohibited from using non-Company Systems, such as their home computers, to engage in such discussions when doing so would: (i) reveal confidential information; or (ii) be defamatory.

Employees should primarily use the Internet for Company-related business. While occasional personal use is permitted, such use must not be excessive and must not interfere with the Company's operation of its Systems. Additionally, even while engaging in occasional personal use, Company policies apply to all use of Company Systems.

Employees and directors are prohibited from using Company Systems to transmit, send, respond or in any way post any document, file, picture, notice, message or other information that does not comply with Company policies and Company standards for ethical and professional conduct.

The Company has software and systems in place that can monitor and record

Internet usage. The Company's security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat room, newsgroup or email message, and each file transfer into and out of the Company's network, and the Company reserves the right to record such information as it, in its sole discretion, deems appropriate.

No employee or director should have any expectation of privacy as to his or her Internet usage through Company Systems.

Transmissions over the Internet may not be secure, and appropriate discretion should be utilized before providing personal information. Employees and directors must exercise caution in revealing their home address, phone number or email address, and must not disclose any such information concerning colleagues without their explicit permission. Special precautions should be taken regarding transmission of financial or credit card information.

12. Audits of the System

To ensure compliance with these policies, the Company may conduct periodic audits of its Systems, including individual personal computers, portable electronic media and backup tapes. Additionally, companies that license software or other System components to the Company may have the right to audit Company and employee or director usage.

Policy Regarding Securities Trading

Radian Group Inc. ("**Radian**") has adopted this Trading Policy to provide assistance in preventing inadvertent violations and avoiding even the appearance of an improper transaction. Except where otherwise noted in this Trading Policy, this Trading Policy applies to all directors, officers, employees, former employees, and former directors (as each term is used in this Code of Conduct and Ethics) of Radian and its subsidiaries and affiliates ("**Covered Persons**"). This Trading Policy supplements the restrictions included in this Code of Conduct and Ethics (in the *Confidentiality* section, subsections 3 and 4 — which include discussion of the definition of material information, Radian's general procedures for disclosing material information to the public, and liability involved in tipping material nonpublic information to others), and must be read in conjunction with those sections of the Code of Conduct and Ethics.

1. General – Insider Trading

No Covered Person may buy or sell securities of Radian while aware of material nonpublic information about Radian, or pass that information on (so-called "**tipping**") to others who may trade. All questions concerning what constitutes "material" or "nonpublic" information should be directed to the General Counsel.

2. Trading Requirements/Restrictions

Preclearance. All transactions in Radian securities by the following persons must be specifically precleared by the General Counsel or the Chief Financial Officer: (1) directors; (2) "executive officers" as such term is defined under the Securities Exchange Act of 1934, as amended (the "**1934 Act**"); (3) all other members of Radian's executive management team (the "**Executive Team**") designated by the Chief Executive Officer; and (4) their spouses, members of their family sharing their household, and other affiliates such as a trust set up for their benefit (all are referred to in this Trading Policy as "**Preclearance Persons**"). The foregoing persons shall be considered Preclearance Persons during the employee's or director's employment or service with Radian and for the period after termination of employment or service while the employee or director remains subject to the reporting requirements under Section 16 of the 1934 Act. Preclearance Persons must contact the General Counsel or the Chief Financial Officer in advance to obtain prior approval of a contemplated trade. Preclearance approval of a transaction is good for two business days after receiving approval as long as the individual does not acquire material nonpublic information during such time. If the trade does not occur within two business days, preclearance must be obtained again before carrying out the trade.

Trading Window Periods. All transactions in Radian securities by the following persons may be made only during an open Trading Window (as defined below): (1) Preclearance Persons, subject to obtaining preclearance described above; (2) Radian employees who have been identified by the Executive Team as having access to material nonpublic

information about Radian in the normal performance of their duties; and (3) their spouses, members of their family sharing their household, and other affiliates such as a trust set up for their benefit.

A "**Trading Window**" will open each fiscal quarter for a three week period, beginning two full trading days after the release of earnings and ending three weeks thereafter. For example, if the first quarter earnings are released before market opens on May 4, then the Trading Window will open on May 6 (two full trading days after the release of earnings) and close on May 27. If the first quarter earnings are released after market close on May 4, then the Trading Window will open on May 7 and close on May 28. In addition, if the last day of the Trading Window falls on a holiday or a weekend, the last day of the Trading Window will be the last business day prior to the end of the Trading Window.

Event-Specific Blackouts. Radian from time to time imposes, through the General Counsel's office, event-specific blackout periods due to material nonpublic developments in Radian's business. These blackout periods always apply to the Preclearance Persons and, in addition, the General Counsel may notify specific additional employees who are involved in the particular matter that they are subject to the blackout period.

Trading Notifications. All Covered Persons are required to notify Radian in writing (on a form approved by Radian, a "Trading Notification") prior to any transaction in Radian securities. In connection with such Trading Notification, each Covered Person shall acknowledge his or her obligations under this Trading Policy and represent that he or she is not in possession, and will not be in possession at the time of such transaction, of any material nonpublic information regarding Radian. The Trading Notification is good for two business days following submission of such notification.

General. The limitations on transactions in Radian securities imposed by this Trading Policy do not apply to automatic savings plan or employee stock purchase plan purchases. The limitations do, however, apply to open-market purchases and sales, market sales of stock received upon the exercise of stock options, elections involving the Radian common stock fund under Radian's 401(k) plan, Benefit Restoration Plan or other Radian plan, and any "reload" of stock options.

3. 10b5-1 Trading Plans

The provisions set forth above regarding Trading Window periods and preclearance are inapplicable to transactions pursuant to a trading plan adopted in accordance with Rule 10b5-1(c) promulgated under the 1934 Act (a "**Trading Plan**"), as long as in each case:

a. A copy of the Trading Plan is filed with the General Counsel not fewer than three days prior to the first transaction under the Trading Plan; and

b. The person for whose benefit the Trading Plan is initiated represents and warrants

to Radian in writing, either in the Trading Plan or at the time of its initiation, that the he or she is not then aware of any material nonpublic information (except that for those individuals subject to the Trading Window, the Trading Plan may only be initiated during an open Trading Window).

4. Certain Prohibited Transactions

Radian considers it improper and inappropriate for any Covered Person while employed by or providing service to Radian (even if not aware of material nonpublic information) and, in addition, during the period after termination of employment or service while a person remains subject to the reporting requirements under Section 16 of the 1934 Act (even if not aware of material nonpublic information), to engage in certain speculative transactions in Radian securities; therefore, the following transactions are prohibited for all Covered Persons:

a. *Short Sales*. Short sales of Radian securities, (i.e., where a person borrows Radian securities, sells them and then buys Radian securities at a later date to replace the borrowed securities, or where a person already has sufficient shares of Radian securities to sell, but does not deliver them until a later date).

b. *Puts and Calls*. Buying or selling puts or calls of Radian securities. A put is a right to sell a specific security at a specific price prior to a set date, and a call is a right to buy a specific security at a specific price prior to a set date. Call options are purchased when a person believes that the price of a security will rise, whereas put options are purchased when a person believes that the price of a security will fall.

Other Hedging Transactions. Certain forms of hedging or monetization transactions allow a person to continue to own securities without the full risks and rewards of ownership. Accordingly, Radian strongly discourages Covered Persons from engaging in such transactions with respect to Radian securities. Any person wishing to enter into such an arrangement must first pre-clear the proposed transaction with the General Counsel and the Chief Financial Officer. Any request for pre-clearance of a hedging or similar arrangement must be submitted to the General Counsel at least two weeks prior to the proposed execution of documents evidencing the proposed transaction and must set forth a justification for the proposed transaction.

5. Post-Employment Trading

This Trading Policy continues to apply to a Covered Person's transactions in Radian securities even after the Covered Person's employment or service with Radian has terminated, as described above. Covered Persons who are aware of material nonpublic information when their employment or service terminates may not trade in Radian securities or disclose the information until the information has become public or is no

longer material.

6. Compliance with Rule 144

Covered Persons who are "affiliates" under federal securities laws are subject to Rule 144 under the Securities Act of 1933, as amended, which establishes certain restrictions on sales of Radian securities, including:

- The amount of Radian securities that such a person may sell within any three-month period can be no more than the greater of: (i) 1% of the total number of outstanding securities of Radian; and (ii) the average weekly trading volume of Radian securities during the four weeks prior to the filing of the related Form 144 or, if such filing is not required, the date a sale order is placed with the broker or the transaction is executed with a market maker;

- Sales must be made through a broker on the open market, generally in unsolicited transactions, or in a transaction directly with a market maker; and

- A Form 144 notice must be filed with the SEC and NYSE to report any sale (including sales pursuant to a Trading Plan) of more than 5,000 shares or of shares with an aggregate value of more than $50,000 during any three-month period.

7. Post-Trade Reporting – Compliance with Section 16

Section 16 of the 1934 Act imposes certain reporting obligations and short-swing trading restrictions on Radian's directors and executive officers. Violations of Section 16 can be costly to individuals and embarrassing to Radian. Under Section 16(b), directors and executive officers must forfeit to Radian any "short-swing" profit deemed to be realized by such insiders on a matched purchase and sale, or sale and purchase, of Radian securities within any six-month period, unless one or both of the transactions are exempt from Section 16(b) liability. Directors and executive officers who fail to report their holdings and transactions in Radian securities in compliance with Section 16(a) are also subject to significant civil fines.

To enable Radian to ensure compliance with Section 16(a), directors and executive officers (including former directors and executive officers while subject to reporting under Section 16) are required to report to the General Counsel or the Chief Financial Officer any transaction in Radian securities (including transactions pursuant to a Trading Plan) by the individual or any immediate family member sharing the individual's household (as well as any trust, partnership or other affiliate through which the SEC attributes "beneficial ownership" to the individual) *immediately* after carrying out the transaction.

8. Personal Responsibility for Compliance; Failure To Comply

All Covered Persons are ultimately responsible for ensuring that they do not violate the insider trading laws or this Trading Policy. Failure to comply with the laws or with this Trading Policy may result in termination of employment or service as well as severe civil and/or criminal penalties.