Woodbury Financial Services, Inc.

Code of Ethics

and

Information Protection Policy

for

Associated Persons

Revised as of January, 07 2013

Woodbury Financial Services, Inc.'s ("Woodbury") Code of Ethics is designed to ensure that principles of honesty, integrity, and fairness are consistently applied to our dealings with clients. Woodbury's reputation is built on these principles. We entrust clients' interests and the firm's reputation every day to each of our employees, representatives and associated persons around the country. Each of us must take care that our actions fully meet our legal duties to our clients. Our clients' interests must always come first; they cannot be compromised.

The heart of Woodbury's Code of Ethics goes to our obligation to remain vigilant in protecting the interests of our clients above our own. The Code of Ethics requires honest and ethical conduct by all employees, representatives and associated persons. Our aim is to be as reasonable as possible with respect to internal procedures, while simultaneously protecting the organization and clients from damage that could arise from a situation involving a real or apparent conflict of interest. While it is not possible to identify all situations in which conflicts might arise, Woodbury's Code of Ethics is designed to set forth certification and disclosure policies in those situations in which conflicts are most likely to develop.

The principles of honesty and accountability are—and have always been—integral to Woodbury's way of doing business. By embracing these principles, we earn the trust of our clients and business partners, a trust that is the foundation of our business. Accordingly, Woodbury requires that each of us behave ethically. We encourage you to become familiar with all facets of our Code of Ethics and trust that you will embrace and comply with both the letter and the spirit of its requirements.

Sincerely,

Rick Fergesen
President & Chief Executive Officer
Woodbury Financial Services, Inc.

Table of Contents

I. Introduction

This Code of Ethics (the "Code") does not, nor is it intended to, address every law, rule or policy. The Code also does not serve as a substitute for using common sense, good judgment, and to obtain additional guidance when needed. Answering the following questions may provide further guidance related to whether any concerns related to the propriety of any action or behavior that may be in conflict or violation of the spirit or letter of the Code should be vetted with a supervisor, human resources representative, or Woodbury's compliance department.

- Will my action comply with the Code and Woodbury's policy or policies at issue?
- Does my action reflect the values of honesty, integrity and respect for individuals?
- Will my action reflect well on me and Woodbury if it becomes known to my co-workers, clients, family and friends or appears on the front page of my local newspaper?

The Code is supplemented by other policies which are referenced throughout this document. Woodbury may change the Code and its related policies without advance notice at any time. Woodbury also retains the sole right to administer and interpret all policies within this Code.

II. Standards of Business Conduct

The following Standards of Business Conduct are applicable to all Associated Persons. Associated Persons are those who have regular access to the keeping, handling, or processing of securities or monies, who have access to the keeping, handling, or processing of the original books and records relating to securities or monies; or non-registered individuals who have a supervisory responsibility over others who engage in any of the activities listed previously.

Compliance with Laws and Regulations

The foundation of our ethical standards is compliance with the letter and spirit of the law. All Associated Persons must respect and obey all applicable federal and state laws and regulations, including those mentioned in other parts of the code. This includes prohibiting any activity which directly or indirectly:

- Defrauds a client in any manner;
- Misleads a client, including any statement that omits material facts;
- Operates or would operate as a fraud or deceit on a client;
- Functions as a manipulative practice with respect to a client; or
- Functions as a manipulative practice with respect to securities.

Ethical Principles

Woodbury is committed to conducting its business according to the highest standards of honesty, integrity and respect for individuals and to demonstrating to our clients, investors, business partners, regulators and government officials that their trust in Woodbury is well deserved. Associated Persons and all business partners are expected to abide by the ethical principles and policies set forth in this Code. The success of Woodbury's compliance program depends upon diligent efforts to comply with this Code. All Associated Persons are expected to perform up to the highest ethical standards and in accordance with applicable laws, rules and regulations.

The Law and Compliance Department as well as the senior executive team are expected to provide advice and guidance and/or identifying the appropriate Woodbury resources for proper advice and guidance on ethics and compliance matters. The Law and Compliance Department and senior executive team must take the lead in: (i) promoting ethical behavior by being open and honest about business conduct, (ii)

fostering working conditions that support ethics and compliance, and (iii) providing a work environment that encourages ethical concerns to be raised and discussed openly without fear of retaliation.

Woodbury strives to create mutually beneficial relationships with its business partners and to promote the application of the ethical standards presented in this Code. Consistent with that objective, Woodbury expects its business partners to perform in accordance with the applicable ethical standards and in accordance with all applicable laws, rules and regulations whenever they transact business with, for, or on behalf of Woodbury.

Bribes

Associated Persons are strictly prohibited from offering, soliciting or accepting bribes. A bribe can be cash or anything of value that is offered or accepted as a "quid pro quo," that is, as part of an agreement to do, or not to do, something in return for the payment or other thing(s) of value.

Compliance and Cooperation with Investigations

When requested to do so, Associated Persons have the duty to cooperate fully with internal, regulatory, and/ or criminal investigations. Associated Persons must be truthful in all dealings with internal, governmental and regulatory investigators, and must not:

(1) Destroy, alter, or conceal any documents or other potentially relevant evidence in anticipation of, or in reaction to, a request from any governmental or regulatory authority or any court,

(2) Lie or otherwise make misleading statements in connection with any federal, state or local government or law enforcement agency investigation, or any internal investigation by Woodbury,

(3) Obstruct, fraudulently influence or impede any external or internal investigation or inquiry or make any improper attempt to do so, or

(4) Attempt to cause any other person or any third party to destroy evidence, to provide false or misleading information or otherwise obstruct any investigation.

The refusal to cooperate constitutes grounds for sanction and disciplinary action up to and including termination of association.

Electronic Communications Policy

All Associated Persons should use care and good judgment when creating all correspondence, voicemail, e-mail, and written documents on behalf of Woodbury to avoid inaccuracy or offensive language. E-mail and voicemail created, sent, received or stored through Woodbury's electronic mail and voice system(s) is the property of Woodbury and is subject to audit at any time. Associated Persons should use only Woodbury approved e-mail for business purposes, with personal usage kept to a minimum. Violation of the Electronic Communications Policy may lead to sanction and disciplinary action, up to and including termination of association with Woodbury.

III. Certification and Disclosure Duties of Associated Persons

Associated Persons must know and understand their disclosure and certification duties under the Code. Failure to comply with these duties can result in sanction and discipline, up to and including termination from association.

Initial and Annual Certification to the Code of Ethics

Associated Persons are responsible for complying with the Code's requirements. Woodbury will ensure that all Associated Persons are provided with copies of the Code and any amendments to the Code. To help ensure compliance with the Code, Woodbury requires periodic certifications regarding receipt of the Code and any amendments to it. Failure to comply with the required certification process or the requirements of the Code will result in appropriate disciplinary action, up to and including termination of association.

Duty to Report Violations

Associated Persons are required to report ***known or suspected*** violations of the Code. Any Associated Person who knows or has reason to believe that an applicable law, rule or regulation or any provision of this Code has been violated is expected to report the violation immediately using one of the methods described below. Failure to take action or simply disregarding a known or suspected violation of law or of any provision of this Code is never appropriate and is itself a violation of the Code. Reporting delays also can increase substantially Woodbury's legal and financial exposure. Woodbury will investigate all reports promptly and confidentially to the extent possible.

Prohibition Against Retaliation

Woodbury prohibits retaliation against any person for reporting an activity that the person, in good faith, believes to be a violation of any law, rule, regulation or provision of this Code. Retaliation against any person is considered a violation of this Code. This provision is meant to protect and encourage reporting known or suspected violations. Further, federal law makes it a crime to retaliate against a person (including with respect to their employment) for providing truthful information to a law enforcement agency or officer relating to the possible commission of any federal crime.

Any person who believes that he/she has been the subject of any form of retaliation related to a reported violation should report the matter directly to Woodbury's Chief Compliance Officer (CCO).

Confidentiality of Reports

Woodbury will take all reasonable precautions to keep the identity of the person reporting a violation confidential. Woodbury's desire to address reported violations with care and discretion is meant to encourage reports of Code violations. However, confidentiality of reported violations shall not apply to reported violations that are determined to be false and presented solely for the purpose of committing an act of libel, defamation, false light, or other fraud with malice or intent to harm.

Associated Persons are encouraged to seek advice from Woodbury's Law and Compliance Department with respect to any action or transaction which may violate the Code and to refrain from any action or transaction that might lead to the appearance of a violation.

Where to Report Violations

Violations of this Code are to be reported as follows:

(1) **Contact the Chief Compliance Officer** by calling Woodbury at 1-800-800-2638. Violations reported are held to the confidentiality standard described within this section.
(2) **Contact the Code of Ethics Hotline** at 651-702-1680. Reports made via the hotline are held to the confidentiality standard described within this section and copies are provided to the Chief Compliance Officer.

Disclosure of Material Conflicts of Interest

Disclosure is required of any other known or anticipated material conflict of interest not otherwise designated in this section and must be disclosed to the Chief Compliance Officer as soon as the conflict situation becomes apparent. Disclosure must include the totality of the known circumstances surrounding

any situation that creates, or appears to create, a conflict of interest. For further information regarding examples of conflicts of interest, see Section IV within this Code.

IV. Conflicts of Interest

Woodbury expects all Associated Persons to exercise sound judgment and to preserve objectivity in business decision-making. Business decisions should be made with the best interest of our clients in mind, solely on the basis of quality service, price and other competitive factors and without the influence of personal bias or conflicts of interest. Associated Persons may not use or abuse a corporate position for personal advantage or promote any actions contrary to Woodbury's interests or ethical standards established in this Code. The guidelines set forth below apply generally to all Associated Persons, but Woodbury may adopt stricter policies as circumstances require.

In order to maintain Woodbury's reputation and integrity, it is the responsibility of every Associated Person to avoid conflicts of interest. A conflict of interest exists where an Associated Person's relationships, financial interests, outside activities or other personal considerations compromise the ability to objectively exercise professional judgment, comply with professional responsibilities or act in the best interest of clients. Associated Persons should also avoid situations involving the potential for a conflict of interest because even the appearance of a conflict can undermine confidence in ethical behavior, and thereby do harm to the reputation of the individual and to Woodbury. The potential for conflicts of interest exists across a wide range of common business activities. Every Associated Person should be aware of the potential for a conflict of interest to arise in his or her own situation and must resolve the issue according to this policy.

The potential for conflicts of interest exists across a wide range of common business activities. The following guidelines are intended to assist Associated Persons in avoiding these conflict situations. Please note that this is not intended to be a comprehensive list of situations in which conflicts may arise. There are many other situations that may also create a conflict of interest. Every Associated Person should be aware of the potential for a conflict of interest to arise in his or her own situation and must resolve the issue according to this policy.

Whether a situation presents an actual or potential conflict of interest is not always clear. Any Associated Person who has any doubt about whether a situation, or course of action, poses such a conflict should immediately consult with his or her supervisor or Woodbury's Law and Compliance Department. In the event a conflict does arise, disclosure of such a conflict in writing to the Chief Compliance Officer is required. To avoid even the appearance of a conflict of interest, Associated Persons should provide full disclosure of any business, financial interest, or involvement in activity that might influence, or appear to have the capacity to influence, the actions or decisions on behalf of Woodbury.

Failure to properly resolve a conflict of interest, or a potential conflict of interest, will result in appropriate disciplinary action.

Use of Corporate Resources

Associated Persons may not, without the consent of the Chief Legal Officer, use Woodbury's name, logo, proprietary information, office space, facilities, staff, vehicles, telephones, computers, copy machines, supplies or any other resources or equipment in connection with outside employment or business activities.

For-Profit Organizations

Associated Persons may not, without the consent of Woodbury's Chief Legal Officer, serve as a member of the board of directors of an outside, for-profit organization.

V. Insider Trading Policy

Woodbury's Insider Trading Policy is designed to prevent the misuse of material non-public information (MNPI). The following procedures have been established to aid Woodbury and all persons in avoiding insider trading, and to aid Woodbury in preventing, detecting, and imposing sanctions against insider trading. Everyone must follow these procedures or risk serious sanctions, including dismissal, substantial personal liability and criminal penalties. Any questions about these procedures should be directed to the CCO.

(1) Before trading securities for yourself or others, including Client accounts, you should ask yourself the following questions:

(a) Is the information material? Is this information that an investor would consider important in making his or her investment decisions? Is this information that would substantially affect the market price of the securities if generally disclosed?

(b) Is the information non-public? To whom has this information been provided? Has the information been effectively communicated to the marketplace by being published in Reuters, The Wall Street Journal or other publications of general circulation?

(2) If, after consideration of the above, you believe that the information is material and non-public, or if you have questions as to whether the information is material and non-public, you should take the following steps:

(a) Report the information and proposed trade immediately to the CCO.

(b) Do not purchase or sell the securities either on behalf of yourself or on behalf of others, including Clients.

(c) Do not communicate the information inside or outside Woodbury, other than to the CCO.

(d) After the CCO has reviewed the issue, you will be instructed either to continue the prohibitions against trading and communication because it has been determined that the information is material and non-public, or you will be allowed to trade the security and communicate the information.

(3) Information in your possession that is identified as material and non-public may not be communicated to anyone, including persons within Woodbury, except as otherwise provided herein. In addition, care should be taken so that such information is secure. For example, files containing material, non-public information should be sealed and access to computer files containing material, non-public information should be restricted, and conversations containing such information, if appropriate at all, should be conducted in private (for example, not by cellular telephone, to avoid potential interception).

(4) If, after consideration of the items set forth above and in background below, doubt remains as to whether information is material or non-public, or if there is any unresolved question as to the applicability or interpretation of the foregoing procedures, or as to the propriety of any action, it must be discussed with the CCO before trading or communicating the information to anyone.

Background- Insider Trading

What are the elements of insider trading?

The purchase or sale of a security of any issuer on the basis of

- Material
- Nonpublic
- Information about that security or the issuer ("MNPI")
- In breach of a duty of trust or confidence
- Owed to the issuer, its shareholders or to any other person who is the source of the information

Who is an insider?

The concept of "insider" is broad. It includes officers, directors and employees of a company. In addition, a person can be a "temporary insider" if he or she enters into a special confidential relationship in the conduct of a company's affairs and as a result is given access to information solely for the company's purposes. A temporary insider can include, among others, a company's attorneys, accountants, consultants, bank lending officers and the employees of such organizations. According to the United States Supreme Court, the company must expect the outsider to keep the disclosed non-public information confidential, and the relationship must at least imply such a duty before the outsider will be considered an insider.

What is material information?

Trading on inside information is not a basis for liability unless the information is material. "Material information" generally is defined as information for which there is a substantial likelihood that a reasonable investor would consider it important in making his or her investment decisions, or information that is reasonably certain to have a substantial effect on the price of a company's securities. No simple "bright line" test exists to determine when information is material; assessments of materiality involve a highly fact-specific inquiry. For this reason, you should direct any question about whether information is material to the CCO.

Material information often relates to a company's results and operations including, for example, dividend changes, earnings results, changes in previously released earnings estimates, significant merger or acquisition proposals or agreements, major litigation, liquidation problems and extraordinary management developments.

Material information also may relate to the market for a company's securities. Information about a significant order to purchase or sell securities may, in some contexts, be deemed material.

Material information does not have to relate to a company's business. For example, in Carpenter v. U.S., 108 U.S. 316 (1987), the United States Supreme Court considered as material certain information about the contents of a forthcoming newspaper column that was expected to affect the market price of a security. In that case, a Wall Street Journal reporter was found criminally liable for disclosing to others the dates that reports on various companies would appear in The Wall Street Journal and whether those reports would be favorable or unfavorable.

What is non-public information?

Information is non-public until it has been effectively disseminated broadly to investors in the marketplace. One must be able to point to some fact to show that the information is generally public. For example, information is public after it has become available to the general public through a public filing with the SEC or some other governmental agency, the Dow Jones "tape," Reuters Economic Services, The Wall Street Journal or other publications of general circulation, and after sufficient time has passed so that the information has been disseminated widely. That information may be publicly available if one

knows specifically where to look does not make the information "public" for securities trading purposes unless it is readily available and broadly disseminated.

When does a duty of trust or confidence exist?

Under SEC Rule 10b5-2, a "duty of trust or confidence" exists in the following circumstances, among others:

- Whenever a person agrees to maintain information in confidence;
- Whenever the tipper and tippee have a history, pattern, or practice of sharing confidences, such that the tippee knows or reasonably should know that the tipper expects that the tippee will maintain its confidentiality; or
- Whenever a person receives or obtains MNPI from his or her spouse, parent, child, or sibling.

What are the differing grounds for liability?

The Classical Theory

- Insiders who owe a duty to the issuer- directors, officers, those who enter into special confidential relationship with company and as a result get access to MNPI because of relationship
- Includes employees, attorneys, accountants, consultants

Misappropriation

- Trading based on MNPI that has been misappropriated from someone other than the issuer in breach of duty of loyalty and confidentiality

Tipping

- "Tippee" (receiver of MNPI) stands in the shoes of tipper if knows or should know that tipper is breaching a duty by tipping/sharing the MNPI

What are the penalties for insider trading?

Penalties for trading on or communicating material, non-public information are severe, both for individuals involved in such unlawful conduct and their employers. A person can be subject to some or all of the penalties below even if he or she does not personally benefit from the violation. Penalties include: (a) civil injunctions; (b) treble damages; (c) disgorgement of profits; (d) jail sentences; (e) fines for the person who committed the violation of up to three times the profit gained or loss avoided, whether or not the person actually benefited; and (f) fines for the employer or other controlling person of up to the greater of $1,000,000 or three times the amount of the profit gained or loss avoided.

Violation of the aforementioned prohibitions is considered misuse of Inside Information and is also subject to the potential Sanctions and Discipline of this Code.

Employees shall seek and follow the advice of the CCO or their assigned Compliance Specialist if there is any question whatsoever about the propriety of entering into a transaction involving potential Inside Information.

Rumors

No person shall originate or circulate in any manner a rumor concerning any security which the person knows or has reasonable grounds for believing is false or misleading or would improperly influence the market price of such security.

VI. Compliance with Other Laws

Woodbury is committed to conducting its business affairs honestly, directly, and fairly. It is Woodbury's intention to comply fully with the laws of all jurisdictions in which it operates and conducts business. Engaging in unfair or dishonest business conduct is a violation of this Code and will negatively affect Woodbury's reputation in the marketplace.

Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act (FCPA) strictly prohibits the use of bribes or illegal payments to any non-United States official, political party or political candidate to obtain or retain business or other improper advantage. Acts prohibited under the FCPA include illegal or questionable client rebates; commercial bribes and kickbacks; financial transactions that involve manipulation of sales, earnings, or other financial data; use of interstate commerce to pay or facilitate payment to any non-United States government official, political party, or political candidate; and keeping inaccurate books and records that attempt to disguise or conceal illegal payments. In addition, the use of any third party agents or intermediaries to facilitate any of the illegal payments or actions described above is strictly prohibited.

Anti-Money Laundering (USA PATRIOT Act)

Woodbury is committed to complying with all applicable laws and regulations aimed at deterring terrorists and other criminals from using our free enterprise system to fund terrorist and other criminal activities, including, the USA PATRIOT Act of 2001. Money laundering is the process of engaging in a financial transaction, or a series of transactions, that involves funds used for or derived from criminal activities. The USA PATRIOT Act makes it mandatory for financial services companies to have an anti-money laundering program that contains four basic components:

(1) Internal Policies, Procedures and Controls;

(2) Designation of an Anti-Money Laundering Compliance Officer;

(3) An Independent Audit Function; and

(4) Ongoing Training for Employees and Licensed Representatives.

Woodbury is committed to ensuring that its anti-money laundering program meets these requirements and that all Associated Persons and Woodbury's business partners comply fully with the laws and regulations designed to combat money laundering and the financing of terrorism.

Under no circumstances may any Associated Person knowingly facilitate or participate in any money laundering activity. Any Associated Person who does so will be subject to severe sanction and disciplinary action. Associated Persons with questions concerning their duties, responsibilities or obligations under Woodbury's anti-money laundering program should contact Woodbury's anti-money laundering Compliance Officer. For more information, see Woodbury's Anti-Money Laundering policy as documented in the Manual. Associated Persons who are aware of, or suspect unusual or fraudulent activity must immediately notify the AML Compliance Officer.

Economic Trade Sanctions/OFAC

Woodbury must also comply with the various economic and trade sanctions programs administered by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"). These sanction programs prohibit a variety of commercial activities with specified countries, including specific rules relating to insurance transactions, as well as specific entities and individuals included on OFAC's list entitled "Specially Designated Nationals and Blocked Persons" which can be found at the OFAC website at http://treas.gov/offices/enforcement/ofac. All Associated Persons must understand the obligations of these

policies to ensure that prohibited transactions do not occur. Any questions concerning any situation that may involve a prohibited transaction should be immediately referred to Woodbury's anti-money laundering Compliance Officer.

VII. Information Protection

Woodbury is an information-based enterprise, dependent upon data to conduct its various businesses. All types of information created or collected to support Woodbury's business operations, including information about employees, business operations and plans, prospects, clients and business partners, constitute information assets of Woodbury. Information assets can exist in electronic, physical or other forms. Associated Persons are responsible for protecting such information assets on behalf of Woodbury. The law and various corporate policies guide management in authorizing access, use or disclosure of information assets. Associated Persons and business partners that are granted access to information assets are accountable for their protection, use and disclosure. They have a responsibility to use and disclose information assets only as necessary to perform their job-related duties. These information protection responsibilities apply to information such as financial data and statistics, which we generate for internal use about our prospects and clients as well as to any confidential information received from third parties.

Associated Persons should not share personal proprietary or confidential prospect, client, or business partner information with persons outside of Woodbury unless authorized in writing to do so. If you have questions about protecting the confidentiality of information belonging to a prospect, client or business partner, please consult with a Woodbury Compliance Specialist. Associated Persons leaving Woodbury, voluntarily or otherwise, are prohibited from removing, copying or disclosing any company, prospect or client information, in whatever form, that is proprietary and/or confidential. Associated Persons must not permit the unauthorized reproduction of software or other copyrighted or trademarked materials, or any other unauthorized use or misuse of any intellectual property belonging to or used by Woodbury. Employees are supported in carrying out these responsibilities by Woodbury's Compliance Department. If you are subject to any nondisclosure agreements which Woodbury has executed, you may not disclose any facts related to such agreement under many federal and state laws.

Competitive Intelligence

Woodbury expects all Associated Persons to comply with all applicable laws in acquiring competitive intelligence and not to engage in theft, blackmail, wiretapping, electronic eavesdropping, bribery, improper inducement, receiving stolen property, threats, or other improper methods. Associated Persons should respect the confidentiality of competitor and business partner information and must not misrepresent who they are or for whom they work in obtaining such information. Associated Persons should notify a Woodbury Compliance Specialist whenever they have received information, either identified as, or that they have reason to believe is, confidential or proprietary from another individual or company. Such confidential information may not be used for any purposes other than the specific purpose(s) agreed to by the party providing that information unless the material is deemed to be information generally available to the public.

Privacy

Woodbury values the trust of its clients and is committed to the responsible management, use and protection of data it maintains about them. Federal and state laws, including Regulation S-P, the Gramm-Leach-Bliley Act, and the Health Insurance Portability and Accountability Act, restrict the ways in which Woodbury can share client information. Woodbury has adopted a privacy policy to comply with these laws. Supervised and Associated Persons are expected to comply.

Customer Confidentiality and Privacy

Associated Persons have access to confidential information about customers and Woodbury. All confidential information must be safeguarded and access should only be granted to individuals who have a legitimate right to it. A breach of confidentiality and privacy can have serious consequences. Each Associated Person is responsible for maintaining the security of all confidential information in his or her possession. Confidential information is defined as:

- Name (Last Name with first name or initial) or company name
- Social Security Number or Tax ID
- Address (including zip and other geocodes)
- Date of Birth or Death
- Telephone Number
- Medical History (Text or coded)
- Credit Card Number(s)
- Bank and Financial Account Numbers
- Policy Numbers
- Drivers License Numbers
- Passport Number
- Employment & Military History
- Employee, Military, or Other Association ID Number
- Income or Other Financial Information
- Payment History
- Credit History
- Mother's Maiden Name
- Health Plan Account Numbers
- Vehicle Identification Numbers
- Medical Device Identification Numbers
- Criminal Conviction Records
- Full Face Photographic Images
- Email address

All associated persons who use or have access to customer information, regardless of their position, location, or relationship with Woodbury are required to comply with Woodbury's Privacy Policy and , SEC Rules regarding the protection and disposal of client records and information.

Associated Persons have a duty to:

- insure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of customer records and information;
- protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer; and
- properly dispose of clients' information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

There are numerous reasons to protect client information: (1) It's good business – Woodbury's reputation, as well as your own business success, depends on securing the privacy of customer personal information; (2) It's required by Woodbury's Privacy Policy; and (3) It's the law – federal and state laws require companies and representatives to maintain client data in a safe and protected environment.

Storage of Confidential Information

There have been numerous technological advancements and changes in the workplace (i.e. email, wireless networks) that raise concern regarding customer confidentiality and private information. Regardless of the methods or equipment used to service customers or maintain information, Associated Persons must use every precaution to ensure privacy of customer information.

Suitable storage of confidential information includes:

- always locking the office when away for more than a few minutes or if the office is located in an area accessible to others;
- locking up sensitive and confidential information in a desk or file cabinet when out of the office;
- storing information in a location appropriate to the client's status ("active" v. "inactive") which is identifiable and available for access by authorized employees, external auditors, regulators, attorneys, and Woodbury as necessary; and
- using a locking device for securing data equipment, including laptops, servers, CPUs, or any other devices containing confidential information.

SEC, FINRA, and State books and record retention requirements have transitioned, or are in the process of transitioning, to electronic means. All persons associated with Woodbury may keep information in electronic format only if it meets the following requirements:

- Saved in a Write Once Read Many ("WORM") format, meaning the information may be viewed many times, but cannot be not be altered once it is saved;
- Private client information is kept secure and confidential (see the following section for additional guidance); and
- Electronic records are backed up at least weekly.

If electronic records are maintained, pursuant to the requirements listed above, the original paper records may be securely destroyed, provided the person confirms that the electronic data has been successfully backed-up, validated and encrypted.

Protecting Electronic Access to Confidential and Private Client Information

Woodbury believes that protecting Client Data is of the utmost importance to serve and protect its clients and representatives. Representatives, Associated Persons, and home office employees are responsible for protecting sensitive information that they handle or come in contact with, and must know what to do if an information security event is suspected.

Each of the following policies and procedures apply to electronic devices that store or access Client Data for **Woodbury Business only** and do not apply to devices used for strictly personal uses and/or outside business activities.

Antivirus

All persons associated with Woodbury are required to install Antivirus protection on any computer used for conducting Woodbury Business. The Antivirus protection must be configured to automatically: (i) search for and download updates daily, and (ii) perform virus scans daily. Virus scans must be completed **after** updates have been applied. The Antivirus protection must be able to document that scans have been run and that the computer is free from Viruses or Spyware. If a Virus or Spyware is identified, Representatives must ensure that the Malware is eliminated from the computer immediately.

Encryption

All persons associated with Woodbury are required to encrypt all computers, servers, PDAs, and Removable Media Storage Devices. The minimum encryption strength is 128-bit Advanced Encryption Standard.

Any email that contains Client Data within an attached file or body text must be encrypted and sent through the AdvisorMail system. Email subject lines may NOT contain Client Data. Encryption through the AdvisorMail system is not automatic and requires the user to manually activate the encryption. Files containing Client Data may only be transferred through an encrypted AdvisorMail email or on encrypted Removable Media Storage Devices.

As a reminder, representatives must back-up client files for business continuity purposes. Only encrypted Removable Media Storage Devices may be used to back up files or to otherwise transfer Client Data.
Learn how to encrypt an email through AdvisorMail (PDF).

Firewalls/Secure Network

All direct and wireless connections to the internet must be firewalled and secure. Associated Persons may **not** use any unsecure internet connection when accessing Client Data. For direct "wired" connections, a properly configured software or hardware firewall must be established to secure the connection. For wireless connections, the wireless hardware (normally a router) should be configured to use WPA or WPA2 encryption. Also note that a properly configured VPN can be established to create a secure encrypted network to have the flexibility to access Client Data from anywhere.

Example: An associated person may not log into an online program using an unsecure internet connection to access Client Data such as the Woodbury Web site (due to its connectivity to applications containing Client Data), or any product manufacturers' Web sites, etc.
Example: Representatives may not use unsecure wireless "hotspots" such as coffeehouses, airports, hotels, etc. when accessing Client Data.

Passwords

All person associated with Woodbury are required to protect all computers and Removable Media Storage Devices with passwords.

All persons associated with Woodbury **may not share passwords** under any circumstances. Any individual, including a Representative, Associated Person, or Non-registered Administrative Assistant, who requires access to Woodbury password-protected systems, must obtain their own personal set of passwords through the protocols established by Woodbury.

Passwords must utilize a combination of at least three of the following elements: (i) eight or more characters, (ii) upper and lower case letters, (iii) numbers, and/or (iv) special characters (examples: $,*,@).

Transmission of Confidential Information

Special care must be used when transmitting confidential information to ensure information security. Ways to securely transmit confidential information include:

- being aware of what is being said and to whom when speaking in a public place;
- holding private conversations in protected and secure places to avoid being overheard;
- knowing when using a cellular or cordless telephone, the security of the transmission cannot necessarily be guaranteed;
- never leaving sensitive or confidential information on voicemail;
- only providing necessary information when corresponding via email or by phone;
- omitting confidential information in electronic communications unless appropriate security mechanisms are in place;
- encrypting all emails that contain confidential customer information, even when sent to Woodbury;

- taking special care to ensure email messages containing confidential customer information are not inadvertently sent to inappropriate parties;
- using the email- and fax-specific disclosure statements detailed in the Required Disclosure Statements section of this Manual;
- only generating hard copies of confidential information to the extent necessary to complete normal business activities and destroyed appropriately once the activity is completed;
- when transferring hard copy confidential information, placing documents in a sealed sensitive/confidential envelope and clearly addressing the intended recipient on the envelope;
- protecting confidential information sent by postal service or courier from unauthorized access or misuse. Representatives and their employees must ensure packaging is sufficient to protect contents from physical damage or tampering. Special controls that may be used include, but are not limited to, tamper resistant packaging, delivery by hand, and signature upon delivery;
- collecting all printed documents containing confidential information from printers, fax machines, and photocopiers immediately; and
- erasing all confidential client information written on whiteboards or work boards after use.

Representatives and Associated Persons are required to use a Woodbury-approved email address when communicating information regarding securities business.

Disposal of Confidential Information

Documents that contain confidential customer information must be shredded or incinerated. These documents must never be placed in the trash or general recycling bins. Electronic information storage devices (i.e. hard drives, tapes, CDs) that contain confidential information must be disposed of in a manner that does not allow for the information stored on the device to be retrieved.

Information Security Events

A large number of data breaches occur from the unauthorized access of hardware or systems. Because of this, many states have enacted statutes that require an institution to notify all impacted clients when a data breach occurs. The notification process is costly, requiring a large amount of resources in a short period of time. Most states, however, waive the client notification requirement if the electronic device lost was encrypted. The encryption of electronic devices is critical to a solid privacy protection plan. Please refer to Encryption for additional information.

Even the most complete and thorough policies and procedures for protecting client data can't protect against lost mail, lost paper documents, laptops being stolen and other mishaps. The remediation and clean-up required after a data breach can be extensive. Woodbury retains the right to pass on costs associated with the remediation of any breach of client data. The assessment of costs will vary given the specific scenario of the breach.

Associated Persons that become aware of an actual, suspected or **potential** Information Security Event must immediately contact the Compliance Department and inform Woodbury's Privacy Officer of the security event. The Privacy Officer can be reached by contacting the Privacy Hotline at (866) 434-3929. Examples of information security events that must be reported include, but are not limited to: (1) loss/theft of a computer or Removable Media Storage Device, (2) hardcopy data loss, (3) inadvertent mailing, email, fax, or disclosure, (4) public display of Client Data, (5) improper document disposal, (6) system break-ins, (7) system virus attacks that cannot be caught and destroyed by the antivirus software, and (8) software or data tampering.

VIII. Investigations and Legal Proceedings

Duty to Report

Associated Persons who receive a demand, complaint, notice or otherwise become aware that Woodbury or one of its licensed representatives is the subject of any legal or administrative proceeding, governmental or regulatory investigation or inquiry, or client complaint, must immediately notify Woodbury's Regulatory Relations Team within the Law Department. This reporting requirement includes, but is not limited to, the receipt of any subpoena or other request for documents or information concerning Woodbury's business operations.

Any Associated Person that becomes aware of a governmental investigation that concerns any business operation within Woodbury must not conduct his/her own investigations. It is the responsibility of Woodbury's Law and Compliance Department to determine whether to conduct an internal investigation, as well as to determine the scope and methods to be employed in conducting any such investigation. Most investigations involve complex legal and business issues and an individual attempting to investigate such matters may compromise the integrity of the investigation. If the results of any internal or governmental investigation warrant corrective action, the Law and Compliance Department will determine the appropriate steps to be taken and will be responsible for implementation of any such remedial or preventative measures.

Participation in an Investigation

All Associated Persons have the duty to cooperate fully with any investigation conducted by Woodbury's Law and Compliance Department. Associated Persons are strongly encouraged to cooperate fully when requested to do so in connection with any law enforcement investigation, subject only to the reporting requirements set forth above. Associated Persons must be truthful in all dealings with internal or governmental investigators, and must not:

(1) Destroy, alter, or conceal any documents or other potentially relevant evidence in anticipation of, or in reaction to, a request from any governmental or regulatory authority or any court;

(2) Lie or otherwise make misleading statements in connection with any federal, state or local government or law enforcement agency investigation, or any internal investigation by Woodbury's Law and Compliance;

(3) Obstruct, fraudulently influence or impede any investigation or inquiry or make any improper attempt to do so; or

(4) Attempt to cause any other Associated and/or supervised person or any third party to destroy evidence, to provide false or misleading information or otherwise to obstruct any investigation.

This Code does not prohibit any person subject to it from providing information or assisting in an investigation in connection with conduct that the Associated Person reasonably believes constitutes a violation of criminal fraud statutes or any rule or regulation of the Securities and Exchange Commission.

IX. Administration and Enforcement of the Code

Training and Education

All Associated Persons are required to read, understand and abide by the Code. It shall be the responsibility of Woodbury's Chief Compliance Officer to implement a Code training program.

New Associated Persons will receive training in the form of written communication on the Code upon association with Woodbury. Associated Persons will also receive additional training in the form of written

communication whenever a new or substantially enhanced version of the Code is adopted. Periodic training may be conducted as necessary. Managers and supervisors are responsible for ensuring that all persons under their supervision have satisfied any required training.

Annual Review

The adequacy of the Code and the effectiveness of its implementation will be reviewed on an annual basis by the Chief Compliance Officer. Any material deficiencies will be escalated to the appropriate members of Woodbury's senior executive team.

Recordkeeping

Woodbury will maintain such books and records relating to this Code including but not limited to:

- A copy of the Code currently in effect and any that have been in effect within the past five years
- A record of any violation of the Code and of any action taken as a result of the violation
- All written acknowledgements of the Code of Ethics for each person who is currently, or within the past five years, were an Associated Person.
- A list of persons who are currently, or within the past five years were, Associated Persons.
- All records documenting the annual review of the Code of Ethics
- All records of any request for pre-approval of investments and the responses thereto
- Any other record or document created pursuant to the Code, including approvals of waivers or exceptions

Discipline and Sanctions

The need to invoke discipline and/or sanctions is necessary to enforce the Code's ethical practice requirements. Appropriate remedial measures will be taken on a case by case basis. Code violations can result in sanctions and disciplinary actions against the Associated Person and the corresponding Licensed Representative including:

(1) verbal warning,
(2) letter of caution,
(3) fine,
(4) suspension,
(5) termination.

In addition to sanctions, violations may result in referral to civil or criminal authorities where appropriate.

Waivers

Waivers or exceptions to the Code will be granted only under exceptional circumstances. Examples include, but are not limited to: acts of God, substantial bodily injury, prolonged illness, or death of a close family member or spouse.

Exceptions to required duties or prohibited practices of this Code may only be made by Woodbury's Chief Compliance Officer or Woodbury's Chief Legal Officer. All requests for exceptions must be made in writing and present adequate proof of the rationale for the waiver request, unless the individual requesting such exception is physically unable to provide such writing. All granted exceptions must be documented in writing and received by the person (or their named delegate) requesting such exception.

Internal Use

Although this Code may be given to prospects, clients, and business partners, the Code is intended solely for internal use by Woodbury and does not constitute an admission, by or on behalf of Woodbury, as to any fact, circumstance, or legal conclusion.

Not a Binding Contract of Employment

The Code and other related policies referenced in this document do not constitute a binding contract of employment between any Associated Person and Woodbury or constitute such ministerial control over any independent contractor to constitute de facto employment or vicarious liability implications.