

PRIVACY POLICY AND PROCEDURES AND PROGRAM FOR PROTECTING CLIENT INFORMATION

Statement of Policy

It is the Firm's policy to protect and safeguard the privacy and security of the personal information the Firm obtains about its "customers" (as that term is defined in Regulation S-P and below). The CCO is responsible for protecting and safeguarding the privacy and security of customer information.

I. Procedures

Information the Firm Collects

The Firm collects certain nonpublic personal identifying information about its customers (such as their name, address, social security number, etc.) from information that the customers provide on applications or other forms as well as communications (electronic, telephone, written or in person) with them or their authorized representatives (such as their attorney, accountant, etc.). The Firm also collects information about their brokerage accounts and transactions (such as purchases, sales, account balances, inquiries, etc.).

Information the Firm Discloses

The Firm does not disclose the nonpublic personal information it collects about its customers to anyone except: (i) in furtherance of its business relationship with them and then only to those persons necessary to effect the transactions and provide the services that they authorize (such as broker-dealers, custodians, independent managers, etc.); (ii) to persons assessing its compliance with industry standards (e.g., professional licensing authorities, compliance consultants, etc.); (iii) its attorneys, accountants, and auditors; or (iv) as otherwise provided by law.

The Firm is permitted by law to disclose the nonpublic personal information about its customers to certain third parties that perform administrative or marketing services on its behalf or for joint marketing programs. These third parties are prohibited from using or sharing the information for any purpose other than for which it was originally provided. If customers decide at some point to either terminate the Firm's services or become inactive, the Firm will continue to adhere to its privacy policy, as may be amended from time-to-time.

Security of Information

The Firm restricts access to customers' nonpublic personal information to those persons who need to know that information to service the customer's account. The Firm maintains physical, electronic and procedural safeguards that comply with applicable federal or state standards. In furtherance of such safeguards, the Firm has adopted an Information Security Policy.

Changes to this Privacy Policy

The Firm's policy about obtaining and disclosing information may change from time-to-time. In all such instances, the Firm will provide its customers with notice of any material change to this policy before implementing the change.

Privacy Notices

The Chief Compliance Officer will ensure that a notice describing the Firm's privacy practices (the "Privacy Policy Notice") is distributed to all customers at the time of the initial formation of the relationship and, thereafter, annually throughout the relationship

Definitions

For the purpose of this section, the following definitions apply:

- Customer relationship: means a continuing relationship between a consumer and the Firm under which the Firm provides one or more financial products or services including advisory services to the consumer that are to be used primarily for personal, family, or household purposes;
- Joint Marketing: A formal agreement between nonaffiliated financial companies that together market financial products or services to individuals;

Opt-Out Notice

If NorthCoast plans to disclose nonpublic personal information (other than pursuant to certain exceptions), NorthCoast will provide consumers and customers a reasonable means to "opt-out" of the disclosure of that information. Once a consumer elects to opt-out, NorthCoast must honor the election as soon as reasonably practicable. The opt-out election remains in effect until the consumer revokes it.

II. Program for Protecting Customer Information

The CCO and his/her designees are responsible for implementing and maintaining the Program.

Identifying Internal and External Risks

The Program is designed to identify foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such customer information. An assessment and evaluation will be made of the likelihood and potential damage of these threats, the sufficiency of any safeguards in place to control such risks and, where appropriate, the Program will be revised to address such risks (the "Risk Assessment"). At a minimum, the Risk Assessment will include a consideration of the risks in each of NorthCoast's areas of operation, including:

- Employee training and management, including instructing and periodically reminding employees of NorthCoast's legal requirement and policy to keep customer information secure and confidential;
- Information systems, including network and software design, as well as information processing, storage, transmission, retrieval and disposal; and
- Detecting, preventing and responding to attacks, intrusions, or other system failures.

Design and Implementation of Safeguards

Information safeguards will be designed and implemented to control the risks identified through the Risk Assessment, and the effectiveness of the safeguards' key controls, systems and procedures will be regularly tested or otherwise monitored.

Overseeing Service Providers

Reasonable steps will be taken to determine that the service providers who have been selected and retained by NorthCoast, at a minimum, maintain sufficient customer information safeguard procedures to detect and respond to security breaches. Moreover, reasonable procedures will be implemented to discover and respond to widely-known security failures by service providers. Finally, all contracts with service providers must contain assurances that such service providers have implemented and will maintain such safeguards.

Evaluation and Maintenance of the Program

The Program will be periodically adjusted, as necessary or appropriate, based on: (i) results of testing and monitoring pursuant to the Program; (ii) any material changes to the business and operation of NorthCoast; and (iii) any other circumstances that may have a material impact on NorthCoast's information security system.