Section 5.0 Privacy Policy & Breach Procedures

The firm recognizes its obligation pursuant to the Gramm Leach Bliley Act (GLBA). Privacy laws regulate what the firm is allowed to do with the confidential personal information that it collects, uses and maintains in connection with its advisory activities, as well as under what circumstances it may share it with someone else.

5.1 Privacy Policy Notice

The firm will ensure that its "Privacy Policy" is provided to its clients not later than the time it establishes a relationship. The CCO will ensure the firm provides privacy notices annually to each client, defines the cyclical reporting period, and that the firm is consistent in applying it to all clients.

5.2 Firm Privacy Policy

The firm will not disclose information outside of the below exceptions. As part of firm policy, confidential personal information will be restricted only to APs who need to know the information to provide advisory services.

Physical, electronic, and procedural safeguards will be maintained to comply with regulatory standards to guard client non-public personal information (NPI). The firm will provide a reasonable means to prevent NPI from being disclosed to non-affiliated parties. The firm will attempt to enter into a written arrangements that require service providers to maintain confidentiality of client NPI.

Clients may opt out of the release of their information, and the firm will not require the client to write a letter to opt out. There are no opt out rights for the release of NPI the firm makes to service providers, however, the firm will disclose to its client via its privacy policy statement the nature of any information to be shared. Opt out rights typically do not apply to disclosure of NPI in the following circumstances:

- Client has consented to and not revoked the disclosure.
- Resolving client disputes or inquiries.
- Personnel holding legal or beneficial interest relating to the client.
- Persons acting in a fiduciary capacity on behalf of the client.
- Providing information to regulatory agencies assessing the firm's compliance with regulations.
- When required to firm legal counsel, consultants, accountants, auditors, etc., in performing their services.

5.3 Cybersecurity Measures

Our firm requires continuous security of firm and client data, and access to such information will be controlled. In coordination with information systems personnel, the CCO will record the following action items on no less than an annual basis:

- Identify in writing internal and external staff having access to firm systems and data.
- APs trained in cybersecurity risks, responsibilities and action steps based on their role.
- Conduct an inventory of all physical systems and devices that are used within the firm. Restrict or eliminate removable or portable media where appropriate.

- Inventory software platforms and applications used by the firm. Correct/update, restrict or eliminate weaknesses involving these platforms/applications.
- Map networks, connections and data flows (including locations where client data is housed) and ensure they are updated. Correct/update, restrict or eliminate weak areas.
- Resources (hardware, data and software) are prioritized for protection based on their sensitivity and business value.
- Catalog connections to the firm's network from external sources. Restrict such access where appropriate.
- Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance.
- Review/update of firm encryption requirements based on systems/devices based and the data utilized.
- Ensure annual business continuity plan testing incorporates cybersecurity threats.
- Create and update vendor inventory to determine types of services, access and potential risks using vendor.
- Request a report from service providers of their assessment of system/control room access to determine validity of physical security plan.
- Request a report from service providers involving penetration tests to determine system weaknesses.
- Review vendor security policies with respect to cybersecurity to determine adequacy or consideration of other providers.

5.4 Identity Theft Protection

The firm's security program is designed to maintain reasonable safeguards to protect personal information of its clients as well as its associates.

Assignment of Data Security Officer

The firm has identified the CCO as the Data Security Officer (DSO) who will be responsible for the policy, oversight, testing and execution of the firm's data security.

Safeguards

The DSO will ensure that policy and action items address administrative, technical and physical safeguards the firm must utilize to protect against a loss of sensitive, non-public personal or firm information.

Risk Assessments

The DSO will take reasonable steps to foresee both internal and external risks to firm and client data. A risk inventory and how risk items are to be addressed will be referenced in a separate working document maintained by the DSO.

Service Provider Agreements

The firm will also provide a reasonable means to prevent NPI from being disclosed to non-affiliated parties. The firm will enter into a written arrangement that requires any service provider to maintain confidentiality of client NPI and sensitive firm information.

5.5 Disposal of Consumer Report Information and Records

NPI records will be disposed in a manner that is designed to prevent unauthorized access or use. Procedures include the following:

- APs will be trained in proper disposal procedures.
- Secure removal of trash involving consumer report information.
- Paper information will be burned, pulverized, or shredded so that it cannot be read or reconstructed.
- Electronic information is destroyed or erased (preferably military-grade protocol) so that information cannot be read or reconstructed.
- Information system hardware (copiers, scanners, printers, PCs, etc.) will not be discarded or donated unless the firm is assured NPI has been eliminated from equipment.

5.6 Breach Procedures

Privacy breaches have the potential to cause adverse impact on the firm, clients, or business partners. In order to respond to a data breach in an efficient, appropriate, timely manner, the firm has established breach response procedures. An important aspect of the firm's response is organizing and initiating the execution of a response to the loss of NPI -- either through an unintentional release or purposeful and unapproved access to secure data.

5.6.1 Breach Planning

Given the types of NPI that may be collected by the firm there is a potentially elevated risk of a data breach. An important first step in responding to a privacy breach is to ensure appropriate contingency planning. To facilitate a timely response to a breach, internal training and awareness are critical.

<u>Identifying Levels of Risk</u>

Each data breach will have a different level of associated risk depending on the data elements compromised.

When determining risk levels, the firm will need to also understand the category of information that has been exposed (i.e., client, AP, etc.). The chart on the following page provides the basis for the protection of data elements. Data elements are separated into three classifications with unique handling requirements and associated risks: Public, Sensitive, and Confidential.

Data Classification	Risk Level	Description	Data Element Examples
Public	Low	Internal or external originating data which the public has access and does not expose an individual to any risk with its release. Authorized parties may circulate such information outside of the organization.	Name, address, and other information commonly found on business cards. Approved marketing materials would also be classified as public.
Sensitive	Moderate	Internal use only content which contains enough proprietary information as to make it imprudent to release to the public.	Corporate policies, employee newsletters, strategic planning information, and employee contact information.
Confidential	High	Internal use content or data accessible only to defined employee groups. Unauthorized disclosure may seriously and adversely impact the firm, client, or business partners. Unauthorized disclosure of this data may lead to regulatory or legal implications.	Passport number, driver license number, SSN/FEIN, personal financial information (i.e. credit card numbers), marital status, and date of birth.

Assessing the Breach: The firm will assess the type of data that had been compromised and all of the circumstances of the data loss, including:

- Level of difficulty for unauthorized persons to access NPI.
- Means in which the loss occurred as well as whether the incident might be the result of criminal activity or is likely to result in criminal activity.
- Evidence that compromised information is actually being used by an unauthorized party.
- Where and how the breach occurred, and when it had been detected.
- Number of individuals possibly affected.
- Types of NPI at risk.

Considering the noted factors together should assist in developing a gauge of where the greatest risk(s) exist, how to proceed, and where to best deploy responses.

5.6.2 Notifications

Following risk level identification and assessment, the firm will implement its response. When the firm has made the decision to provide notice to those at risk, it may incorporate the following into the process:

Timing of Notification: Notice provided in a timely and appropriate manner. It must not be done hastily based on incomplete facts or in a way that may exacerbate the situation. While it is important and often legally required to promptly notify those who may be affected, false alarms are counterproductive. The CCO may consider consulting legal counsel or industry consultants regarding the timing and content of any announcement before making any public disclosures.

Coordination with Ongoing Investigations: Under certain circumstances law enforcement may require a temporary delay before notice is given to ensure that criminal investigations may effectively be conducted (i.e., international hacking ring, etc.).

Method of Notification: Given the serious security and privacy concerns raised by data breaches, notification to affected individuals should be issued in a controlled manner by selected parties. The firm will consider the best method of notification given the type of breach and number of individuals affected, as well as its regulatory obligation. Various methods may include website postings, mailings, email, or phone calls.

Content of Notification: The notice should be concise and easily understood. The following items should be considered for inclusion into the notice:

- Brief description of what occurred.
- A description of the types of NPI involved in the breach.
- Brief description of what the firm is doing to investigate the breach, mitigate loss, and protect against further breaches.
- Key contacts and procedures for additional questions or to learn more information.
- Steps individuals should take to protect themselves from the risk of identity theft, including steps to take advantage of any credit monitoring or other service the firm or its provider will offer.

Notifying Government Agencies and/or Credit Agencies: Various state laws require certain commissioners or credit agencies be notified in some or all situations. Depending on the legal requirement, number of individuals affected, and types of data elements possibly exposed, credit reporting agencies or local government offices may need to be notified of the breach in addition to the individual. Governmental or regulatory body notifications will be completed by the CCO or legal counsel.

Post Notification Considerations: Once affected individuals and authorities have been notified, the firm will prepare for additional inquiries. APs will be briefed on the incident and provided prepared responses to questions.