# Client Privacy

---

**Issue**

The SEC's Regulation S-P (Privacy of Consumer Financial Information), which was adopted to comply with Section 504 of the Gramm-Leach-Bliley Act, requires investment advisers to disclose to clients, who are natural persons, its policies and procedures regarding the use and safekeeping of client records and Non-public Personal Information.

Non-public Personal Information is collected from clients at the inception of their accounts and occasionally thereafter, primarily to determine accounts' investment objectives and financial goals and to assist in providing clients with requested services.

Examples of Nonpublic Personal Information includes: name, address, phone number (if unlisted), social security and tax identification numbers, financial circumstances and income, and account balances.

**Risks**

In developing this policy and procedures, SUMMIT GLOBAL INVESTMENTS, LLC considered the material risks associated with protecting Non-Public Personal Information. This analysis includes risks such as:

- Information about Clients/Investors is not maintained or used in ways that ensures such information is safe from unauthorized use.
- Employees' use of email and the internet is not properly monitored for inappropriate use.
- Email and other electronic communication with clients (instant messaging, Facebook, etc.) are not maintain, as required by the book and records rule.
- Employees are not aware that their use of the internet, email, and social media (Instagram, face book, etc.) are subject to the same standards as all other forms of communication and is not private.
- Regulatory documents are delivered electronically without the client's informed consent to receive such documents electronically.
- SGI's service providers do not adequately safe guard Client Information.

**Policy**

SGI will not disclose a client's Non-public Personal Information to anyone unless it is permitted or required by law, at the direction of a client, or is necessary to provide requested services.

**Procedures**

1. SGO shall not sell Non-public Personal Information to anyone.

2. SGI will restrict access to Non-public Personal Information to individuals within SGI who require the information in the ordinary course of servicing clients' accounts. Clients' Non-public Personal Information is used only for business purposes.

3. SGI has developed procedures to safeguard client records and Non-public Personal Information. (See Attachment A).

4. Non-public Personal Information may only be given to third-parties under the following circumstances:

    - To broker/dealers to open a client's brokerage account;
    - To other firms as directed by clients, such as accountants, lawyers, etc;
    - To specified family members (as authorized by law and/or the client);
    - To third-parties as needed to provide requested services, and
    - To regulators and others, when required by law.

5. At times, Non-public Personal Information may be reviewed by SGI's outside service providers (i.e. – accountants, lawyers, consultants, etc.). SGI will review the entities' privacy policies to ensure that client's information is not misappropriated or used in a manner that is contrary to this privacy policy.

6. SGI shall provide the Privacy Notice to clients (i.e. "natural persons") upon inception of the relationship and annually thereafter. SGI will maintain a record of the dates when the Privacy Notice is provided to clients.

7. In the event of a change in the Privacy Policy, SGI will provide its clients with a sufficient amount of time to opt out of any disclosure provisions.

8. Any suspected breaches to the Privacy Policy must be reported to the Chief Compliance Officer

9. If an Employee receives a complaint regarding a potential identity theft issue (be it from a client or other party), the Employee should immediately notify the Chief Compliance Officer. The Chief Compliance Officer will thoroughly investigate any valid complaint and maintain a log of all complaints as well as the result of any investigations.

10. In the event that unintended parties receive access to Client Information, SGI will discuss the matter with Outside Counsel and promptly notify those clients/investors of the privacy breach as might be necessary.

11. In the event that unintended parties receive access to Non-public Personal Information of California residents, SGI will promptly notify those clients of the privacy breach.

**Responsibilities**

The Chief Compliance Officer will monitor for compliance with SGI's Privacy Policy and Procedures and will coordinate the dissemination of the Privacy Notice.

**Attachment A**

**Procedures to Safeguard Client Records and Non-public Personal Information**
SGI shall strive to: (a) ensure the security and confidentiality of consumer, customer and former customer records and information; (b) protect against any anticipated threats or hazards to the security or integrity of consumer, customer and former customer records and information; and (c) protect against unauthorized access to or use of consumer or customer records or information that could result in substantial harm or Inconvenience to any customer. Accordingly, the following procedures will be followed:

A. Confidentiality. Employees shall maintain the confidentiality of information acquired in connection with their employment with SGI, with particular care taken regarding Non-Public Personal Information. Employees shall not disclose Non-Public Personal Information, except to persons who have a bona-fide business need to know the information in order to serve the business purposes of SGI and/or Clients. SGI does not disclose, and no Employee may disclose, any Non- Public Personal Information about a Client or former Client other than in accordance with these procedures.

B. Information Systems. SGI has established and maintains its information systems, including hardware, software and network components and design, in order to protect and preserve Non- Public Personal Information.

   *Passwords and Access*. Employees use passwords for computer access, as well as for access to specific programs and files. Non-Public Personal Information shall be maintained, to the extent possible, in computer files that are protected by means of a password system secured against unauthorized access.

   Access to specific SGI databases and files shall be given only to Employees who have a bona-fide business need to access such information. Passwords shall be kept confidential and shall not be shared except as necessary to achieve such business purpose. User identifications and passwords shall not be stored on computers without access controls, written down, or stored in locations where unauthorized persons may discover them. Passwords shall be changed if there is reason to believe the password has been compromised and, in any event, changed periodically (i.e., at least once every 90 days) to maximize the Security of Non-Public Personal Information. All access and permissions for terminated Employees shall be removed from the network system promptly upon notification of the termination.

   To avoid unauthorized access, Employees shall close-out programs and shut-down their computers when they leave the office for an extended period of time and overnight. Terminals shall be shut- down when not in use during the day and laptops shall be secured when leaving SGI premises. Confidentiality shall be maintained when accessing the SGI

network remotely through the implementation of appropriate firewalls and encrypted transmissions.

*System Failures*. SGI will maintain appropriate programs and controls (which may include anti- virus protection and firewalls) to detect, prevent and respond to attacks, intrusions or other systems failures.

*Electronic Mail*. As a rule, Employees shall treat e-mail in the same manner as other written communications. However, Employees shall assume that e-mail sent from SGI computers is not secure and shall avoid sending e-mails that include Non-Public Personal Information to the extent practicable. E-mails that contain Non-Public Personal Information (whether sent within or outside SGI shall have the smallest possible distribution in light of the nature of the request made.

*Disposal*. Electronic media, on which Non-Public Personal Information is stored, shall be formatted and restored to initial settings prior to any sale, donation, or transfer of such equipment.

C. Documents. Employees shall avoid placing documents containing Non-Public Personal Information in office areas where they could be read by unauthorized persons, such as in photocopying areas or conference rooms. Documents that are being printed, copied, or faxed shall be attended to by appropriate Employees. Documents containing Non-Public Personal Information which are sent by mail, courier, messenger, or fax, shall be handled with appropriate care. Employees may only remove documents containing Non-Public Personal Information from the premises for bona-fide work purposes. Any Non-Public Personal Information that is removed from the premises must be handled with appropriate care and returned to the premises as soon as practicable.

D. Discussions. Employees shall avoid discussing Non-Public Personal Information with, or in the presence of, persons who have no need to know the information. Employees shall avoid discussing Non-Public Personal Information in public locations, such as elevators, hallways, public transportation, or restaurants.

E. Old Information. Non-Public Personal Information that is no longer required to be maintained shall be destroyed and disposed of in an appropriate manner. Refer to the Document Destruction procedures contained in the Maintenance of Books and Records policy for additional information.

F. Identity Theft. An identity thief can obtain a victim's personal information through a variety of methods. Therefore, Employees shall take the following actions to prevent identity theft:

1. When providing copies of information to others, Employees shall make sure that non-essential information is removed and that Non-Public Personal Information which is not relevant to the transaction is either removed or redacted.

2. The practice of *dumpster diving* provides access for a would-be thief to a victim's personal information. Therefore, when disposing of paper documents, paperwork containing Non- Public Personal Information shall be shredded, burned or otherwise destroyed.

3. To avoid a fraudulent address change, requests must be verified before they are implemented, and confirmation notices of such address changes shall be sent to both the new address and the old address of record.

4. Employees may be deceived by *pretext calling*, whereby an "information broker" or "identity thief" posing as a Client, provides portions of the Client's Non-Public Personal Information (i.e., Social Security Number) in an attempt to convince an Employee to provide additional information over the phone, which can be used for fraudulent purposes. Employees shall make every reasonable precaution to confirm the identity of the Client on the phone before divulging Non-Public Personal Information.

5. SGI prohibits the display of Social Security Numbers on any documents that are generally available or widely disseminated (i.e., mailing lists, quarterly reports, etc.).

Employees could be responsible for identity theft through more direct means. Insider access to information could permit a dishonest Employee to sell Non-Public Personal Information or to use it for fraudulent purposes. Such action is cause for disciplinary action at SGI's discretion, up to and including termination of employment as well as referral to the appropriate civil and/or criminal legal authorities.