Client Privacy

Implementation Date: March 1, 2005

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 its policies and procedures regarding the use and safekeeping of 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.

While Helios Wealth Advisors, LLC (HWA) strives to keep client information up to date, clients are requested to monitor any information provided to them for errors.

For purposes of this policy, "Non-public Personal Information" means:

- personally identifiable financial information, including any information a client provides to obtain a financial product or service; any information about a client resulting from any transaction involving a financial product or service; or any information otherwise obtained about a client in connection with providing a financial product or service to that client; and

- any list, description, or other grouping of clients (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available information.

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

Policy

HWA 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. HWA shall not sell Non-public Personal Information to anyone.

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

3. HWA 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 HWA's outside service providers (i.e. – accountants, lawyers, consultants, etc.). HWA will review the entities' privacy policies.

6. HWA shall provide a privacy notice (See Attachment B) to clients (i.e. "natural persons") upon inception of the relationship and annually thereafter. HWA 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, HWA 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 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 Compliance Officer. The Compliance Officer will thoroughly investigate any valid complaint, and maintain a log of all complaints as well as the result of any investigations.

Responsibilities

The Compliance Officer will monitor for compliance with HWA'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

Helios Wealth Advisors, LLC (HWA) 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 HWA, with particular care taken regarding Nonpublic Personal Information. Employees shall not disclose Nonpublic Personal Information to other HWA Employees, except to persons who have a bona-fide business need to know the information in order to serve the business purposes of HWA or its clients. HWA 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. HWA 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. All Employees use passwords for computer access, and may do so for access to specific programs and files. Nonpublic Personal Information shall be maintained, to the extent possible, in computer files that are protected against access by means of a password system or are otherwise secured against unauthorized access. Access to specific HWA databases and files shall be given only to Employees who have a bona-fide business need to access such information. Such passwords shall be kept confidential and shall not be shared except as necessary to achieve such business purpose. All default user identifications and passwords that may be provided shall be changed and replaced by distinct passwords which may be easily remembered by the Employee but difficult for others to guess. User identifications and passwords shall not be stored on computers without access control systems, 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., once every 90 days) to maximize the security of Non-public Personal Information. To avoid unauthorized access, all Employees shall close out programs and lock their terminals when they leave the office for an extended period of time and overnight. Terminals shall be locked when not in use during the day and laptops shall be secured when leaving HWA premises. Confidentiality shall be maintained when accessing the HWA network remotely through the implementation of appropriate firewalls. Files may be accessed and shown only to those individuals authorized on a "need to know" basis.

System Failures. HWA 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 HWA computers is

not secure and shall avoid sending e-mails that include Non-public Personal Information except as specifically set forth above. E-mails that contain Non-public Personal Information (whether sent within or outside HWA) shall have the smallest possible distribution in light of the nature of the request made.

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 photo-copying 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 NOT REMOVE NON-PUBLIC PERSONAL INFORMATION IN ANY FORMAT/MEDIUM (INCLUDING HARD COPY DOCUMENTS AND COMPUTER DISKS) FROM THE PREMISES WITHOUT THE PERMISSION OF THE CCO. ANY NON-PUBLIC PERSONAL INFORMATION THAT IS REMOVED MUST BE HANDLED WITH APPROPRIATE CARE.

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 not discuss Nonpublic Personal Information in public locations, such as elevators, hallways, public transportation or restaurants.

E. Access to Offices and Files. Employees shall limit access to offices, files or other areas where Nonpublic Personal Information may be discussed or maintained, and shall enter such locations for valid business purposes only. Meetings with clients shall take place in conference rooms or other locations where Non-public Personal Information will not be generally available or audible to others. Visitors shall generally not be allowed in the office unattended.

F. Old Information. Nonpublic Personal Information that is no longer required to be maintained shall be destroyed and disposed of in an appropriate manner.

G. 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:

a) 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.

b) The practice of *dumpster diving* provides access for a would-be thief to a client's personal information. Therefore, when disposing of paper documents, paperwork containing Non-public Personal Information shall be shredded.

c) 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.

d) Employees may be deceived by *pretext calling*, whereby an "information broker" or "identity thief" posing as an investor, provides portions of the investor'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.

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

Employees may be responsible for identity theft through more direct means. Insider access to information allows a dishonest Employee to sell consumers' personal information or to use it for fraudulent purposes. Such action is cause for disciplinary action at HWA's discretion, up to and including termination of employment as well as referral to the appropriate civil and/or criminal legal authorities.

Attachment B

Privacy Notice

This notice is being provided to you in accordance with the Securities and Exchange Commission's rule regarding the privacy of consumer financial information ("Regulation S-P"). Please take the time to read and understand the privacy policies and procedures that we have implemented to safeguard your nonpublic personal information.[5]

INFORMATION WE COLLECT

Helios Wealth Advisors, LLC (HWA) must collect certain personally identifiable financial information about its customers to provide financial services and products. The personally identifiable financial information that we gather during the normal course of doing business with you may include:

1. information we receive from you on applications or other forms;

2. information about your transactions with us, our affiliates, or others;

3. information we receive from a consumer reporting agency.

INFORMATION WE DISCLOSE

We do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted or required by law, or as necessary to provide services to you. In accordance with Section 248.13 of Regulation S-P, we may disclose all of the information we collect, as described above, to certain nonaffiliated third parties such as attorneys, accountants, auditors and persons or entities that are assessing our compliance with industry standards. We enter into contractual agreements with all nonaffiliated third parties that prohibit such third parties from disclosing or using the information other than to carry out the purposes for which we disclose the information.

CONFIDENTIALITY AND SECURITY

We restrict access to nonpublic personal information about you to those Employees who need to know that information to provide financial products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal standards to guard your nonpublic personal information.

---

[5] Nonpublic personal information means personally identifiable financial information and any list, description or other grouping of consumers that is derived using any personally identifiable financial information that is not publicly available.