

PRIVACY REQUIREMENTS

Regulation S-P was issued by the SEC in June 2000 in response to the privacy requirements of the *Gramm-Leach-Bliley Act of 1999* (“*GLB Act*”). Regulation S-P is a comprehensive set of SEC rules that are focused on preventing financial institutions from disclosing various types of non-public personal information gathered from individual clients to unaffiliated persons. Regulation S-P prohibits the sharing of non-public personal information with any non-affiliated third party unless the firm has provided notices of its privacy policies and “opt-out notices” allowing clients to “opt-out” of the disclosure of such information. The types of personal information covered generally include any information that is not already publicly available but is provided by a client in order to obtain financial products or information from an adviser providing services or engaging in transactions for the client.

The *GLB Act* permits states to enact privacy protections that are stronger than those contained in the *GLB Act* and Regulation S-P. In order to further meet the privacy concerns of their residents, California, Connecticut, Massachusetts, New Mexico, and Vermont have enacted privacy protections which are stronger than the provisions of the *GLB Act* and Regulation S-P. With regard to clients who are residents of these states, RetireWise is prohibited from sharing non-public personal information with a non-affiliated third party, not in connection with providing advisory services, unless the firm has provided notices of its privacy policies and “opt-in” notices allowing clients to “opt-in” to the disclosure of such information. An “opt-in” generally requires RetireWise to obtain from its client and consumers a signed statement in which the person makes an affirmative declaration of permission to disclose certain personal information.

RetireWise is required to adopt policies and procedures designed to protect various records and information it maintains about its natural person clients. It is required to provide “clear and conspicuous” notices reflecting its privacy policies and procedures to a client initially at the time a relationship is established and annually thereafter. The initial notice must be provided at the time the client enters into an advisory contract with RetireWise. Any initial notice may be provided within a reasonable time after it establishes a client relationship if: (i) establishing the client relationship is not at the client's election, (ii) providing notice no later than when the client relationship is established would substantially delay the client's transaction and the client agrees to receive the notice at a later time, or (iii) a non-affiliated broker or dealer establishes a client relationship between the adviser and a consumer without the adviser's prior knowledge.

For purposes of Regulation S-P, an individual who is the record holder of a fund's shares is considered the client. If the client has multiple accounts, RetireWise is permitted to deliver a single Privacy Notice provided the notice makes it clear which accounts it applies to and the client can reasonably be expected to receive the actual notice regarding each account.

RetireWise's Privacy Notice will include, at a minimum, the following:

- A general description of its policies and procedures to protect the confidentiality, security and integrity of clients' non-public personal information;
- Categories of clients' non-public personal information collected;
- Categories of clients' non-public personal information disclosed;

- If applicable, categories of affiliates or non-affiliated third parties that may receive the information; and
- If applicable, an explanation of a client's right to opt out or opt in and the method used to exercise that right

In certain circumstances, RetireWise is permitted to share client non-public personal information with non-affiliated third parties without providing the client notice of and an opportunity to opt out. Such circumstances include sharing information:

- With a non-affiliate if necessary to effect, administer, or enforce a transaction that a client requests or authorizes
- In connection with processing or servicing a financial product or service a client authorizes
- In connection with maintaining or servicing the client's account with the institution.

Under these exceptions, RetireWise does not need to provide the client the opportunity to opt out or opt in before sharing the client's non-public personal information with a non-affiliated broker/dealer in order to execute trades the client has authorized with a non-affiliated custodian that holds securities on behalf of the client.

Jonathan Vogel is responsible for maintaining RetireWise's Privacy Notice and all required records pertaining to such document. Jonathan Vogel will be responsible for training supervised persons and making sure everyone is aware of and complies with RetireWise's Privacy Notice policies and procedures. Jonathan Vogel will be responsible for ensuring that all clients receive the initial delivery and annual delivery of RetireWise's Privacy Notice.

INFORMATION SECURITY PLAN

Pursuant to Rule 30 of Regulation S-P, RetireWise has adopted the following Information Security Plan to address the administrative, technical, and physical safeguards for the protection of client records and information. The purpose of this information security plan is to ensure the security and confidentiality of client personal information, protect against any anticipated threats or hazards to the security of client information, and protect against the risk of identity theft.

Personal information is considered a person's first and last name, or their first initial and last name, in combination with their Social Security number, driver's license number or state issued identification card number, or their financial account number or credit or debit card number. Personal information does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records that are available to the general public. The personal information collected by RetireWise will be limited to what is reasonably necessary to accomplish business purposes or to satisfy regulations. Further, access to personal client information will be limited to those supervised persons required to know such information.

To protect clients' personal information, RetireWise has implemented the following physical security safeguards:

- **Entrances** - All entrances/exits are secured;
- **Visitors** - All visitors are required to check-in at central location and only allow visitor access to office areas with confidential client information on an escorted basis;
- **Servers** – Servers and/or server room is locked and limited to key personnel;
- **Alarm System** – A security service or alarm system for office is utilized during non-business hours;
- **Employee Background Checks** - Background checks are conducted on new employees including unlicensed staff;
- **Vendor Background Checks** – Vendors with access to offices (e.g., Maintenance & janitorial services) are required to conduct background checks of workers;
- **Paper Files** - Client files are physically locked during non-business hours;
- **Shredding Paper Records** - Shredding is required when disposing of any paper records which reference to confidential client information; and
- **Suspicious Information** - Employees are encouraged to report suspicious or unauthorized use of confidential client information.

To protect clients' personal information, RetireWise has instituted the following safeguards:

- Client files are physically locked during non-business hours;
- Strong electronic passwords are utilized that:
 - Contain alphanumeric/special character combinations;
 - Require users to change the password after a certain time period; and
 - Lock the device after several unsuccessful attempts at access
- When disposing of old computers, hard drives, and other storage medium are removed and physically destroyed;
- Whenever possible, alternatives are used in place of social security numbers and account numbers;
- Any email request for client information or to change client information must be sent using DMARC;
- Wireless connections (WEP/WPA) are password protected;
- At least annually, RetireWise will employ a qualified professional to conduct a security audit; and
- Passwords are never provided by email or through a web page accessed through a link in an email.

In addition, supervised persons of RetireWise are required to:

- Put away open client files when leaving their desk;
- Shred documents when disposing of physical files;
- Never share their electronic passwords;

- Set electronic devices to require users to re-login after a period of inactivity;
- Encrypt all client information transferred or stored on portable electronic devices such as laptops, tablets, external hard drives, CD-ROMs, disks, thumb drives, and smart phones; and
- Utilize and update patches for operating systems, firewalls, and anti-virus and malware software for business computers, and personal electronic devices used for business purposes.

To limit outside access to confidential client information via the use of smart phones, each supervised person is required to password protect his or her smart phone and set the auto-lock function for the shortest possible time. The auto-lock function of the smart phone should also be set to clear the smart phone's memory after a set number of failed log-in attempts or to automatically power down the phone.

To further protect the confidentiality of clients' personal information, all visitors to RetireWise's office are restricted to one entry point for each building in which personal information is stored. In addition, visitors will be required to present a photo ID, sign in, and wear a plainly visible "Guest" badge or tag. At no time will visitors be permitted in any area of RetireWise's office where client personal information is stored or accessible, unless the visitor is escorted by an supervised person of RetireWise.

In the event of termination, a supervised person must return all records containing any form of client personal information. This includes all information stored on laptops or other portable devices or media, and information stored in files, records, work papers, etc. The terminated supervised person's physical and electronic access to personal information of clients will be immediately blocked and the terminated supervised person will be required to surrender all keys, IDs, access codes, or badges that permit access to RetireWise's premises or information. In addition, the terminated supervised person's remote electronic access to personal information will be disabled and his or her voicemail access, email access, internet access, and passwords will be invalidated.

Jonathan Vogel is in charge of RetireWise's information security. Accordingly, Jonathan Vogel is responsible for training supervised persons, testing and regularly monitoring the security program, conducting an annual review of the effectiveness of the information security plan, conducting a review whenever there is a material change in the business practices of RetireWise that may implicate the security or integrity of clients' personal information, and conducting training for all individuals who have access to clients' personal information.

Any outside service provider who does business with RetireWise must contractually agree to keep confidential any non-public confidential client information. Jonathan Vogel will conduct due diligence of any service provider used by RetireWise to ensure the service provider's ability to protect client information. (See the Due Diligence section of this manual for more details).

SECURITY BREACH

Supervised persons should report any suspicious or unauthorized use of client information to Jonathan Vogel. Jonathan Vogel will be responsible for conducting a reasonable investigation to determine whether a security breach occurred and the likelihood of the information being misused.

In the event of a security breach, RetireWise will assess the breach and identify which systems and the types of information that were compromised. The firm will then take steps to contain and control the breach and to prevent further unauthorized access or use. Jonathan Vogel will notify clients of the breach if misuse has occurred or it is reasonably possible that misuse will occur. Further, Jonathan Vogel will provide notice to the SEC or the proper state securities authority.

Jonathan Vogel will prepare and archive a report of each Security Breach including when the breach occurred, the information stolen, and an explanation of the steps taken to prevent a reoccurrence of the breach.