Privacy Policy

Introduction

Advisers are subject to federal and state privacy statutes enforced by the SEC, the Federal Trade Commission and certain state regulators and may be subject to foreign privacy laws and data protection regulations with respect to foreign clients. The Firm must collect certain personally identifiable financial information about each client in connection with such client's advised by the Firm. The Firm has established the following guidelines to effectuate and monitor the Firm's Privacy Policy.

Issues

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 individuals who are consumers or customers, their policies and procedures regarding the use and safekeeping of personal information.

The Firm collects personal information from clients at the inception of the client/investor relationship and occasionally thereafter, primarily to determine their investment objectives and financial goals. The Firm also collects personal information from clients in connection with their investment in the Funds. While the Firm strives to keep client/investor information up to date, clients/investors are requested to monitor any information provided to them for errors.

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

- any information an individual provides to obtain a financial product or service (for example, name, address, income, Social Security number, or other information on an application);
- any information about an individual obtained from a transaction involving a financial product/s or service/s (for example, the fact that an individual is a client or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
- any information obtained about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report).
- 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.

NPI does not include information that you have a reasonable basis to believe is lawfully made "publicly available." In other words, information is not NPI when you have taken steps to determine:

- that the information is generally made lawfully available to the public; and
- that the individual can direct that it not be made public and has not done so.

For example, while telephone numbers are listed in a public telephone directory, an individual can elect to have an unlisted number. In that case, her phone number would not be "publicly available."

Additionally, Regulation S-P requires financial institutions to adopt written policies and procedures to properly dispose of sensitive consumer information. The amendments are designed to protect consumers against the risks associated with unauthorized access to information and mitigate the possibility of fraud and related crimes, including identity theft.

Regulation S-AM ("Reg S-AM") prohibits a registered investment adviser from using information about an individual consumer that has been obtained from an affiliated entity for marketing purposes unless the information sharing practices have been disclosed and the consumer has not opted out.

State Privacy Laws – Massachusetts Law 201 CMR 17.00

In addition to Regulation S-P and Regulation S-AM, certain states have adopted consumer privacy laws that may be applicable to Advisers with clients who are residents of those states. For example, Massachusetts has a law (201 CMR 17.00) that requires any company with personal information about its residents to adopt and implement a comprehensive information security program. Advisers that collect information from such residents must incorporate these standards into compliance policies.

Security Breaches

Nearly all states have adopted data breach rules which require financial institutions to implement policies to be alert to, investigate, and provide notice to resident individuals whose personal information is compromised in a security breach. Notification may also be required to regulatory authorities or consumer agencies.

Policy

The Firm will not disclose any client's Non-public Personal Information to any third party unless it is permitted or required by law, at the direction of a client or as necessary to provide the Firm's services.

Supervised Persons must maintain the confidentiality of information acquired in connection with their employment or contract, with particular care being taken regarding Non-public Personal Information. Improper use of the Firm's proprietary information, including Non-public Personal Information, is cause for disciplinary action, up to and including termination of employment for cause and referral to appropriate civil and criminal legal authorities.

Procedures

- The Firm will not sell client information to anyone. Non-public Personal Information is used only for business purposes of the Firm and its affiliates.
- The Firm will restrict access to clients' Non-public Personal Information to individuals within the Firm who require the information in the ordinary course of managing the client's account(s)
- The Firm should seek to limit the amount of Non-public Personal Information obtained from clients to only such information that is necessary.
- To the extent practicable, Supervised Persons should seek to redact nonessential Non-public Personal Information from information disclosed to third parties. Social security numbers should never be included in widely distributed lists or reports.
- Documents set for destruction that contain any Non-public Personal Information or sensitive consumer information shall be disposed of in an authorized recycling container and destroyed.
- Supervised Persons should take reasonable precautions to confirm the identity of individuals requesting Non-public Personal Information. Supervised Persons must be careful to avoid disclosures to identity thieves, who may use certain Non-public Personal Information, such as a social security number, to convince a Supervised Person to divulge additional information. Any contacts with suspected identity thieves must be reported promptly to the CCO.
- The Firm has developed an Information Security Policy & Procedures to safeguard client records and other confidential information.

- The Firm's client information may only be given to unaffiliated third parties under the following circumstances:
    - To other investment managers, custodians, broker/dealers, and other service providers necessary for servicing 1900 Wealth client account(s);
    - To regulators, when and as required by law.
- At times, client information may be reviewed by the Firm's outside service providers (*e.g.,* accountants, lawyers, and consultants). With regard to the Firm's client's information, the Firm will require such entities to have a Confidentiality Agreement with the Firm that generally provides for notification in the event of a security breach the impacts such information, as well as industry standard privacy policies in place that comply with relevant state regulations. If the service provider receives access to EU personal data, contractual guarantees may be mandatory. These guarantees must meet applicable data protection laws, such as the GDPR, which sets out detailed requirements.
- The Firm shall provide a privacy notice (in substantially the form of Notice of Privacy Policy) to each client or prospective client as an exhibit to the subscription documents and in the event the privacy notice changes thereafter, will deliver an updated notice. The privacy notice shall be furnished to clients in a written format and the Firm will maintain a record of the dates when the privacy notice is provided to clients.
- Clients acknowledge receipt of the initial Privacy Notice when executing the investment management agreement. The Firm will provide clients with prompt notice of any material change to the Firm's privacy policies and will give clients sufficient opportunity to opt out of any new disclosure provisions.
- Any suspected breaches of the privacy notice or privacy policy must be immediately reported to the CCO and will be dealt with pursuant to applicable law.
- The majority of states in the U.S. have passed laws requiring notification of any breaches of privacy that occur that may affect citizens of the states. Therefore, in the event that unintended parties receive access to personal and confidential information of clients, the Firm will notify all affected clients.

Privacy Protection Training

All new Supervised Persons should receive, review, and understand their obligations to protect Non-public Personal Information. The CCO will periodically also remind Supervised Persons of their privacy obligations. The CCO may provide training more frequently and/or in person to individuals or groups if:

- The Firm's policies and procedures, or the threats to Non-public Personal Information, change in a material way;
- The Firm experiences a privacy breach; and/or
- One or more Supervised Persons do not appear to understand their obligations regarding privacy protection.

All current Firm Supervised Persons have signed a Confidentiality Agreement and such agreements are maintained in the human resources files. Further and as practicable, each new Supervised Person will be required to sign a Confidentiality Agreement on their first day of work.

Responsibilities

The CCO, or designee, will administer and monitor for compliance with the Firm's Privacy Policy. The CCO oversees the distribution of Privacy Notices and maintains a record of the dates and recipients of Privacy Notices.

Attachment A: Notice of Privacy Policy

1900 WEALTH

Rev.12/2024

FACTS

WHAT DOES 1900 WEALTH MANAGEMENT, LLC DO WITH YOUR PERSONAL INFORMATION?

Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share and protect your personal information. Please read this notice carefully to understand what we do.

What?	The types of personal information we collect and share depend on the product or service you have with us. The information can include: • Social Security number • Account Balances • Payment History • Transaction or loss history • Account transactions • Checking account information When you are no longer our customer, we continue to share your information as described in this notice.

How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons 1900 Wealth Mgmt chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does 1900 Wealth Mgmt share?	Can you limit sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s) respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – to offer our products and services to you	No	We do not share the customers' personal information
For joint marketing with other financial companies	No	We do not share the customers' personal information
For our affiliates' everyday business purposes – information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes – information about your creditworthiness	No	We do not share the customers' personal information
For our affiliates to market to you	No	We do not share the customers' personal information
For our non-affiliates to market to you	No	We do not share the customers' personal information

Questions?	Call (210) 736-7770

Who we are	
Who is providing this notice?	1900 Wealth Management, LLC

What We Do	
How does 1900 Wealth Management protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We also maintain other physical, electronic and procedural safeguards to protect this information and we limit access to information to those employees for whom access is appropriate.
How does 1900 Wealth Management collect my personal information?	We collect your personal information, for example, when you • Open an account • Seek advice about your investments • Apply for financing • Give us your contact information • Show your driver's license We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.
Why can't I limit all sharing?	Federal law gives you the right to limit only: • Sharing for affiliates' everyday business purposes – information about your creditworthiness • Affiliates from using your information to market to you • Sharing for nonaffiliates to market to you State law and individual companies may give you additional rights to limit sharing. See below for your rights under state law.

Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. • *Our affiliates include financial companies such as Jefferson Bank and Sanger & Altgelt, an insurance agency.*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. • *1900 Wealth Management does not share customer information with nonaffiliates for marketing purposes.*
Joint Marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. • *1900 Wealth Management does not engage in joint marketing.*

List of Affiliates

- Jefferson Bank
- Sanger & Altgelt, LLC – Insurance and Risk Management Services

Other Important Information

If our Privacy Policy is expected to change, we will notify you in advance. Your custodian has provided a copy of their Privacy Policy to you in a separate mailing. You may lodge a complaint with a data protection authority for your country or region or where an alleged infringement of applicable data protection laws occurs at https://edpb.europa.eu/about-edpb/board/members_en