Rev. 06/2026

FACTS

WHAT DOES HORIZON FINANCIAL 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. This information can include:

- Social Security number and retirement assets
- Account balances and transaction history
- Investment experience and risk tolerance

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 Horizon Financial chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Horizon Financial share?	Can you limit this 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	Yes	No
For joint marketing with other financial companies	No	No
For our affiliates' everyday business purposes— information about your transactions and experiences	No	No
For our affiliates' everyday business purposes— information about your creditworthiness	No	No
For nonaffiliates to market to you	No	No

Questions? Call 585-334-3600 or go to https://horizonfinancial.net

Who we are

Who is providing this notice?	Horizon Advisory Services, d/b/a Horizon Financial

What we do

How does Horizon Financial 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.
How does Horizon Financial collect my personal information?	We collect your personal information, for example, when you ■ Open an account or provide account information ■ Give us your contact info or seek advice about your investments ■ Enter into an investment advisory contract
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 laws and individual companies may give you additional rights to limit sharing.

Definitions

Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ■ *Horizon Financial has no affiliates.*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ■ *Horizon Financial does not share with nonaffiliates so they can market to you.*
Joint marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ■ *Horizon Financial doesn't jointly market.*

Other important information

HORIZON FINANCIAL

PRIVACY POLICY

Effective June 3, 2026

OUR COMMITMENT TO YOU

At Horizon Advisory Services, your privacy is important to us. We collect, use, retain, and share nonpublic personal information and customer information only as needed to deliver financial advice, manage investments, service accounts, operate our business, protect against fraud or unauthorized activity, and meet legal or regulatory obligations. We do not sell your personal information. We may use your information to tell you about our own services; this is different from sharing your information with unaffiliated third parties for their marketing, which we do not do. We maintain physical, administrative, and technical safeguards, a written incident response program, and secure disposal procedures to protect your information.

SCOPE OF THIS POLICY

This Policy describes how Horizon collects, uses, shares, safeguards, retains, disposes of, and responds to incidents involving nonpublic personal information and customer information under SEC Regulation S-P. Customer information may include information about you that we receive from you, from custodians or other financial institutions, or from vendors that support your accounts, whether in paper, electronic, or other form.

This Policy is intended to describe Horizon's privacy, information-security, disposal, and incident-response practices for clients and prospective clients. The Firm may also provide a separate Regulation S-P privacy notice, including the SEC model privacy form, for initial or annual privacy notice purposes.

Some customer information is sensitive customer information because, alone or in combination with other information, its compromise could create a reasonably likely risk of substantial harm or inconvenience. Examples include Social Security numbers or taxpayer identification numbers; government identification numbers; account numbers; usernames; access codes; security codes; security questions and answers; dates or places of birth; mother's maiden name; biometric information; and similar authentication or account-access information.

Information We Collect

To provide investment advisory services, we collect non-public personal information from a variety of sources, including:

- Account applications and other forms you submit
- Your communications with us (email, meetings, calls, or client document uploads)
- Transaction history and balances from custodians and other financial institutions
- Financial goals, income, risk tolerance, and investment preferences
- This may include, but is not limited to:
- Name, address, phone number(s), and email address(es)
- Date of birth and driver's license number
- Social Security number or taxpayer identification number
- Account information, including holdings at other institutions
- Assets, liabilities, income, and expense data
- Investment activity, experience, and stated goals

We use this information only as reasonably necessary to provide financial advice, manage investments, service accounts, operate our business, protect against fraud or unauthorized activity, and comply with legal and regulatory obligations.

We also may maintain information after an advisory relationship ends as required or permitted by law, and we protect and dispose of former-client information under the same safeguards described in this Policy.

How We Use and Share Your Information

We use your personal information to deliver advisory services, maintain your accounts, fulfill regulatory requirements, and communicate with you about your financial plan or investments.

We may share your information with third parties in the course of providing these services, including:

- Custodians and financial institutions where your accounts are held
- Technology platforms and administrative vendors that support account management, reporting, and communication
- Compliance consultants, legal counsel, or auditors, when needed
- Government agencies or regulators, when legally required

Whenever possible, we share only the specific information required for the third party to perform its role. We do not blanket-share all client information across platforms. However, some systems may require broader access to account data in order to function properly.

We oversee service providers that can access customer information and review their privacy and security practices before and during the relationship. Where commercially feasible, we seek contractual or other written assurances that service providers protect customer information and notify us as soon as possible,

but no later than 72 hours after becoming aware of a breach in security resulting in unauthorized access to a customer information system maintained by the service provider, when required under amended Regulation S-P.

We do not sell your personal information, and we do not share it for marketing or advertising purposes.

We also may share information with your consent, to process or service transactions, to protect against fraud or unauthorized transactions, to respond to regulators, courts, or law enforcement, or as otherwise permitted or required by law. We apply the same policies to information about former clients.

How We Protect Your Information

We safeguard your personal information and customer information using a combination of physical, administrative, and technical controls that are appropriate for a firm of our size and consistent with regulatory expectations. Our practices include:

- Password-protected systems with screen locks and session timeouts
- Multi-factor authentication where supported
- Cybersecurity training for employees
- Physical file storage in locked cabinets (though physical records are limited)
- Document destruction through a professional shredding service, including locked shred bins, restricted access, and a certificate of destruction
- Review of vendor privacy and security practices for key technology platforms
- Customer information system inventory, access reviews, and incident escalation procedures
- Secure backups and business continuity/recovery planning
- Service provider oversight and security reviews

Employees may access customer information only as needed to perform their responsibilities, and access is not extended to non-essential personnel.

Digital Tools and Website Privacy

We use third-party tools to monitor basic website traffic and performance, such as how often visitors return and which pages they view. These tools may collect information such as your device type, IP address, or browser characteristics through cookies or similar technologies. We do not use this data for advertising, and we do not sell or share it for marketing purposes.

We do not currently respond to Do Not Track signals, and our website's behavior remains unchanged when this setting is used.

If you send us documents or personal information through an encrypted upload tool, we retrieve and store the materials in accordance with our retention and security procedures and remove or archive external copies when permitted by the platform and applicable retention requirements. Communications sent by

email or other digital platforms are retained and stored in accordance with applicable regulations and our firm's data retention policies.

We review the privacy and security practices of key technology vendors prior to implementation to help ensure client data is handled responsibly.

Data Retention and Disposal

We retain your personal information and customer information only as long as necessary to provide services, comply with legal and regulatory requirements, and support our business operations. When information is no longer needed and is not subject to a legal or regulatory retention requirement, we dispose of it securely.

Physical records are stored in locked cabinets and are shredded by a professional document destruction service on a scheduled basis. Shredding bins remain locked until pickup, and we receive a certificate of destruction for each job. Access to these bins is restricted and monitored.

Digital records are stored on secure internal systems and retained in accordance with books and records regulations. We periodically review and update our data storage systems so outdated or unnecessary data is removed, archived, or disposed of securely when permitted by law.

Client Rights and Controls

We respect your right to understand how your personal information is used and to control how you hear from us. You may contact us at any time to:

- Update or correct your personal information
- Ask questions about how your data is handled or protected
- Request that we stop sending certain types of communications
- Raise a concern about any aspect of our privacy practices

We make every effort to respond to requests promptly and in a manner consistent with our regulatory obligations and internal policies. To contact us, please call the Chief Compliance Officer at (585) 334-3600, email mrcongdon@horizonfinancial.net, or write to Horizon Advisory Services, Inc., Attn: Chief Compliance Officer, 5582 West Henrietta Road, West Henrietta, New York 14586.

Data Incident and Breach Notification

We maintain procedures to evaluate and respond to potential data incidents. If we become aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred, we will activate our incident response program, assess the nature and scope of the incident, identify affected systems and information, take steps to contain and control the incident, and determine

whether sensitive customer information was or is reasonably likely to have been accessed or used without authorization.

If sensitive customer information was or is reasonably likely to have been accessed or used without authorization, we will provide clear written notice to affected individuals as soon as practicable and no later than 30 days after becoming aware of the unauthorized access or use, unless after a reasonable investigation we determine that the information has not been and is not reasonably likely to be used in a manner that would result in substantial harm or inconvenience, or unless a legally permitted delay applies.

When notice is required, the notice will describe the incident in general terms, identify the type of sensitive customer information involved, include the incident date or estimated date/date range if reasonably possible, provide contact information sufficient to permit you to inquire about the incident, including a telephone number, email address or equivalent method, postal address, and the specific office or contact available to assist you; recommend that you review account statements and immediately report suspicious activity; explain what fraud alerts are and how to place them; recommend that you periodically obtain credit reports from each nationwide credit reporting company and have fraudulent information deleted; explain how to obtain a free credit report; and include information about Federal Trade Commission and usa.gov identity-theft resources and how to report identity theft to the FTC. If a service provider experiences an incident involving customer information, we will initiate our incident response procedures and remain responsible for ensuring required notices are provided.

Summary of How We Share and Your Choices

We do not sell your personal information or share it with third parties for marketing purposes. We share your information only:

- To provide services you've agreed to
- To comply with legal and regulatory requirements
- With vendors or custodians who support your accounts

You cannot limit sharing that is necessary to service your account, maintain your relationship with us, process transactions, or meet legal or regulatory obligations. Because we do not share your information in a way that requires an opt-out under Regulation S-P, this Policy does not include an opt-out election.

Changes to This Policy

We review and update our privacy policy as needed to reflect changes in our business practices or regulatory obligations. If we make material changes, we will notify you and provide an updated copy of this policy.

Our current policy is to provide this notice annually. If the Firm elects to rely on the Regulation S-P annual notice exception in the future, we will do so only when permitted by law and when our information-sharing practices have not changed in a way that requires a revised notice.