PZENA Investment Management

# Privacy/Regulation S-P Compliance

## Revised November 2025

POLICY

Pzena Investment Management[1] ("PIM") is committed to safeguarding the private information of its clients. In accordance with Regulation S-P, 17 CFR 248, we have established this policy and supporting procedures to ensure our practices protect any such information in our possession, including oversight of service providers with access, and responsible disposal protocols. We have implemented an incident response program to ensure effective detection, response, recovery, and notification capabilities. We inform our clients of our privacy practices with an initial notice at relationship inception, and an updated notice when there are changes in our policies or practices regarding the disclosure of nonpublic personal information (consistent with statutory exceptions to annual notices). We also maintain records to evidence the effectiveness of our program in compliance with applicable regulations.

REGULATION

Title V of the Gramm-Leach-Bliley Act of 1999 (the "GLB Act") requires financial institutions to protect the security and confidentiality of their consumers' personal financial information. Regulation S-P adopted by the Securities and Exchange Commission ("SEC"), implements the requirements of Title V with respect to the securities activity of U.S. registered broker-dealers, investment advisers, and investment companies, regardless of whether their clients are U.S. or foreign persons. The Federal Trade Commission adopted privacy rules which are substantially similar to Regulation S-P covering private funds.

In May 2024, the SEC amended Regulation S-P (as amended, the "Regulation") to enhance protection for customer data, with a compliance deadline for larger covered financial institutions of December 3, 2025. The changes included application of the Regulation to transfer agents, a broader definition of "customer information," expansion of the disposal rule, stricter requirements for overseeing service providers, and guidelines for incident response and customer notifications.

REQUIREMENTS

1. **Privacy Notices:** Delivery of an initial and annual privacy notice, explaining how nonpublic personal information will be shared with third parties. PIM provides an initial privacy notice at the beginning of a relationship, but is exempt from the requirement to send annual privacy notices, provided it does not (i) share information with non-affiliated third parties outside the exceptions set forth under the Regulation, or (ii) make substantive changes to its policies or practices regarding the disclosure of nonpublic personal information. PIM shall notify customers of changes to its policies or practices relating to sharing such information as required under the Regulation.

[1] In this policy, the terms "we," "our" and "us" refer to Pzena Investment Management, LLC ("PIM").

2. **Opt-Out:** Consumers must have a clear and easy way to opt out of having their nonpublic personal information shared with non-affiliated third parties. However, PIM is exempt from this requirement since it limits such sharing to applicable exceptions under the Regulation. If we change our practices to allow for information sharing outside such exceptions, we will amend our policy and provide opt-out options for clients in accordance with the Regulation.

3. **Safeguards Rule:** Written policies and procedures must address administrative, technical, and physical safeguards to protect against anticipated threats and unauthorized access. In addition to this policy, PIM addresses safeguards for its systems and data in its *Information Technology & Cybersecurity Policy*, and other privacy obligations and procedures in its *Data Protection Policy*, *Privacy Procedure*, and its *Data Protection Impact Assessment Procedure*.

4. **Disposal Rule:** Safeguards extend to the proper disposal of sensitive consumer information. In addition to this policy, PIM addresses safeguards for disposal of data and technology in its *Information Technology & Cybersecurity Policy* and its *Decommissioning Procedures*.

5. **Incident Response Plan**: Develop and maintain written policies and procedures to detect, respond to, and recover from unauthorized access to consumer information. In addition to this policy, PIM maintains a *Cybersecurity Incident Response Plan* to marshal its process for (i) assessing the nature and scope of an incident; (ii) determining the systems and customer information that may have been affected; (iii) containing and controlling the incident; and (iv) providing customer notice.

6. **Incident Notification**: Affected individuals must be notified as soon as practicable, but no later than 30 days after the institution becomes aware of a breach involving their "sensitive customer information," which is defined under the Regulation to include personally identifiable information. Under our *Cybersecurity Incident Response Plan*, PIM requires notice of breaches of sensitive customer information in accordance with the Regulation.

7. **Service Provider Oversight**: Implement policies and procedures to oversee service providers that have access to customer information, including conducting due diligence and monitoring to ensure service providers maintain safeguards and report privacy breaches within 72 hours. In its policies and procedures, PIM requires oversight of applicable service providers, including prompt notice of privacy issues consistent with the Regulation. In addition to this policy, PIM maintains a *Best Execution Policy* for selection and oversight of brokers/dealers and a *Vendor Management Policy* which requires heightened diligence and oversight of service providers that have access to sensitive customer information.

8. **Recordkeeping**: Maintain written records of compliance, including incident response, service provider oversight, and records of any detected breaches and the subsequent notification process. In addition to this policy, PIM maintains a *Books & Records Policy* which commits PIM to maintain all records required for investment advisers under 17 CFR 275.204-2, including subsection a.25 which mandates maintenance of records covering safeguarding of customer information and incident response plans.

DEFINITIONS

**The Regulation does not prohibit our "affiliated"[2] companies from sharing information with each other but does impose limits on sharing information with non-affiliated third parties.**

Under the Regulation we must protect our "Consumers" and "Customers."

A ***Consumer*** is defined as an individual (or his or her legal representative) who provides nonpublic personal information in seeking to obtain investment advisory services that are to be used primarily for personal, family, or household purposes, even if we ultimately do not provide services to that individual. An individual is not a Consumer if he or she provides only his or her name, address, and general areas of investment interest in connection with a request for an investment adviser brochure (e.g., a prospective Customer) nor is the individual a Consumer merely because he or she is a beneficiary of a trust or sponsored employee benefit plan for which PIM is the trustee or fiduciary.

*A* ***Customer*** is defined as a Consumer who enters into a transaction with us and there is some measure of continued service following, or in connection with, that transaction (e.g., who has an investment advisory contract with us and obtains investment advice).

Shareholders of the mutual funds we advise or subadvise (each, a "Fund", and collectively, the "Funds") are consumers and customers of the Fund itself, not its investment adviser or subadviser. Shareholders of PIM proprietary funds are Consumers and Customers of PIM and this policy and the Regulation would apply. It is the responsibility of our Chief Compliance Officer ("CCO") to ensure we determine the status of everyone with whom we do business.

**Customer Information** means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic or other form, that is in PIM's possession or that is handled or maintained by PIM or on its behalf regardless of whether such information pertains to: (i) individuals with whom PIM has a Customer relationship; or (ii) the customers of other financial institutions where such information has been provided to PIM.

**Customer Information Systems** means the information resources owned or used by PIM, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of customer information to maintain or support PIM's operations.

**Disposal** means: (i) the discarding or abandonment of Consumer or Customer Information; or (ii) the sale, donation, or transfer of any medium, including computer equipment, on which Consumer or Customer Information is stored.

[2] For purposes of the Regulation, an "affiliate" of a financial institution is a company that controls, is controlled by, or is under common control with the financial institution. "Control" is defined as the power to exercise a controlling influence over the management or policies of a company, whether through ownership of securities, by contract or otherwise. The definition of "affiliate" under the Regulation differs from that under the 1940 Act. For purposes of the 1940 Act, a greater than 25 percent (25%) security holder of a company is deemed to have control of such company and to be an affiliate of the same.

The Regulation protects the privacy of **Nonpublic Personal Information** ("**NPI**") about *individuals (including IRAs and family trusts or other estate planning vehicles)* who obtain financial products or services primarily for personal, family, or household purposes. The Regulation does not protect information about: (i) institutional clients (including trusts, partnerships, corporations or employee benefit plans); or (ii) individuals who obtain financial products or services primarily for business, commercial, or agricultural purposes. However, PIM has determined to extend to institutional clients through its general confidentiality policies and procedures certain privacy protection concepts which are described in Section C below.

NPI includes **Personally Identifiable Financial Information** ("**PIFI**") as well as any list, description, or other grouping of Consumers that is derived using any PIFI that is not publicly available information. PIFI is defined as any information: (i) a Consumer provides to obtain a financial product or service (such as name, tax identification number, address and other information provided by a client on our New Account Form); (ii) about a Consumer resulting from any transaction involving a financial product or service between PIM and a Consumer (such as the terms of our investment advisory agreement with a client, client account performance data, client account balances and client account portfolio composition); and (iii) we otherwise obtain about a Consumer in connection with providing a financial product or service to that Consumer (such as information we may obtain about a client from financial consultants, or information about client transactions we may obtain from brokers).

PIFI includes: (i) the fact that an individual is or has been one of our clients or has obtained a financial product or service from us; and (ii) information about our client if it is disclosed in a manner that indicates the individual is or has been our client, including a client list.

PIFI does not include information that does not identify a client, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses. Publicly available information includes any information PIM reasonably believes is lawfully made available to the public from: (i) federal, State, or local government records; (ii) widely distributed media; or (iii) disclosures to the general public that are required to be made by federal, State, or local law.

**Sensitive Customer Information** means any component of Customer Information alone or in conjunction with any other information, the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. This includes Customer Information uniquely identified with an individual that has a reasonably likely use as a means of authenticating the individual's identity, such as (i) a Social Security number, official State- or government-issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (ii) a biometric record; (iii) a unique electronic identification number, address, or routing code; (iv) telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)); or Customer Information identifying an individual or the individual's account, including the individual's account number, name or online user name, in combination with authenticating information such as information described above, or in combination with similar information that could be used to gain access to the customer's account such as an access code, a credit card expiration date, a partial Social Security number, a security code, a security question and answer identified with the individual or the individual's account, or the individual's date of birth, place of birth, or mother's maiden name.

***Service Provider*** means any person or entity that receives, maintains, processes, or otherwise is permitted access to Customer Information through its provision of services directly to PIM.

RESPONSIBILTY

PIM has designated its Chief Compliance Officer ("CCO") responsible for maintaining this policy in compliance with applicable rules and regulation, and has authorized its CCO to enforce this policy and the procedures set forth hereunder. PIM's Chief Information Officer ("CIO") and Manager of Information Security ("MIS"), in consultation with the CCO and Crisis Management team, shall oversee PIM's incident response plan. These officers are also responsible for ensuring PIM maintains copies of all applicable materials, including records of incident investigations and notice delivery, in accordance with applicable recordkeeping requirements. This policy and the accompanying procedures are to be reviewed annually, and any substantive modifications shall require approval of the CCO.

Protecting the private information of PIM's clients is the responsibility of every PIM employee. The CCO (or delegee) should be consulted if there is any ambiguity regarding the categorization of public/nonpublic information. Employees are reminded that all external enquiries regarding client information, even simple confirmation of client identity, should be directed to the CCO or President if there is any doubt as to the public nature of the information and/or authorization to share such information with non-affiliated third parties. Employees violating these policies will be subject to appropriate disciplinary action.

PROCEDURES

## A. Privacy Notices

Under the Regulation, PIM is required to send "Privacy Notices" to its Customers and, in certain cases, to its Consumers. The rules for sending out Privacy Notices may vary depending on whether an individual is a Consumer or a Customer. Our notice discloses how we collect, use, and disclose Customer and Consumer Information. Our notice is provided at the beginning of the relationship and, in accordance with an exemption to annual delivery under the Regulation, when we change our policies or practices for sharing such information. The Regulation was amended to codify a statutory exception to providing an annual Privacy Notice provided that certain conditions are met. Specifically, an entity can be exempt from delivery of an annual Privacy Notice if the entity (i) only provides non-public personal information to non-affiliated third parties when an exception to third-party opt-out applies and (ii) the entity has not changed its policies and practices for disclosing non-public personal information from its most recent disclosure sent to Customers.

**1.** The Privacy Notice must disclose the following information:

(a) the categories of NPI we collect;

(b) the categories of NPI we disclose;

(c) the categories of affiliates and non-affiliated third parties to whom we disclose NPI (other than those to whom we disclose NPI under certain exceptions as described below under section B.1. - *Exceptions to Opt-Out Notice and/or Privacy Notice Requirements*);

(d) the categories of NPI about our former Customers that we disclose and the categories of affiliates and non-affiliated third parties to whom we disclose NPI about our former Customers, other than those parties to whom we disclose NPI under section B.1. below;

(e) the categories of third parties with whom we have contracted to perform services or functions on our behalf and the categories of NPI we disclose to such third parties;

(f) an explanation of the individual's right (if applicable) to "Opt-Out" of non-exempt disclosures to non-affiliated third parties, and how the individual may exercise that right (see section B – *Opt-Out Notice* below);

(g) a general description of our policies and practices designed to protect the confidentiality and security of NPI; and

(h) if we disclose NPI to non-affiliated third parties under section B.1. below, a statement that PIM discloses NPI to non-affiliated third parties in the ordinary course of business to certain financial intermediaries to process transactions, maintain account(s), in response to court orders and legal investigations, or otherwise as permitted by law.

Attached as **Exhibit A** is a form of Privacy Notice that we have adopted ("PIM Privacy Notice").

**2.** Under the Regulation, we may freely share NPI with PIM affiliates, as long as we disclose this practice in a Privacy Notice to our Customers. If we want to disclose NPI to a non-affiliated third party, we must either provide our Customers and/or Consumers with a right to opt-out of that disclosure (see section B below) or make such disclosure under one of several exceptions in the Regulation (see section B.1. below). Thus, it is important to determine whether the recipient of NPI is an affiliate or a non-affiliated third party.

3. PIM maintains a list of affiliates that it is permitted to freely share information by law. The Funds that PIM advises or subadvises are not affiliates because PIM lacks the relevant control of such Funds. However, the Funds are permitted to share their shareholders' non-public information with PIM because of our contractual investment advisory relationship with the Funds. We are obligated to use that information for purposes of providing such services only and for no other purpose. We must treat such information as confidential and safeguard against its disclosure; however, we have no initial or annual notice obligations with respect to the consumers and customers who have provided such information to the Fund.

4. PIM must provide (i) an initial Privacy Notice to each individual who becomes a Customer, which should be provided no later than when PIM establishes a Customer relationship with the individual, and (ii) an annual Privacy Notice, which must be provided to each Customer at least once every 12 months should we no longer qualify for the exemption to annual delivery. The form and content of the initial Privacy Notice and annual Privacy Notice will typically be the same absent amendments to the form (see **Exhibit A**).

5. We endeavor to provide an initial Privacy Notice to a Customer at a point when the individual still has a meaningful choice about whether to enter into a Customer relationship with PIM. Generally, this will occur when we deliver Part 2 of our Form ADV and/or our new client pack and before an investment advisory contract is signed. The following are methods by which we can provide a Privacy Notice:

   (i) Hand-deliver a printed copy of the Privacy Notice to the Consumer or Customer;

   (ii) Mail a printed copy of the Privacy Notice to the Consumer at last known address;

   (iii) Electronic methods:

   - If the Consumer or Customer uses a web site to access financial services and/or his or her account and agrees to receive Privacy Notices at the web site, post the Privacy Notice in a clear and conspicuous manner (e.g., place it on a screen that Consumers and Customers frequently access or place a link on the screen that connects directly to the Privacy Notice and is labeled appropriately to convey the importance, nature and relevance of the Privacy Notice); or
   - Deliver the Privacy Notice with a monthly or quarterly statement.

6. If two or more individuals jointly have a joint account (e.g., a husband and wife), we may provide one Privacy Notice to those individuals jointly. Finally, householding (i.e., delivering a single Privacy Notice to Customers who share the same address but who have two or more separate accounts) is permitted only with respect to *annual* Privacy Notices, provided that: (i) the document is delivered to members of the same family with the same last name sharing a common home address or post office box; (ii) the persons involved are given advance notice of the householding and (iii) the persons involved do not object to the householding.

The CCO is responsible for determining the timing and method of delivering Privacy Notices, and for developing systems and procedures to ensure that the above-mentioned delivery requirements are satisfied.

## B. Opt-Out Notice

"Opt-Out" means a direction by an individual that we not disclose NPI about that individual to a non-affiliated third party, other than as permitted by exceptions in the Regulation described under section B.1. below. If we intend to disclose NPI to non-affiliated third parties beyond these exceptions, we must provide Opt-Out Notices to Consumers and Customers in a manner that is clear and conspicuous, and that accurately explains the right to Opt-Out. As of the date of this Policy, PIM shares NPI with non-affiliated third parties only within the scope of the permitted exceptions. If PIM subsequently identifies a need to share NPI with non-affiliated third parties beyond those exceptions, PIM shall promptly notify its Consumers and Customers and shall advise them as to procedures for complying with the Opt-Out requirements under the Regulation.

### 1. Exceptions to Opt-Out Notice and/or Privacy Notice Requirements

The following three exceptions in the Regulation permit us to share NPI with non-affiliated third parties without having to provide an Opt-Out Notice to Consumers and Customers. The CCO at PIM is responsible for assessing PIM's arrangements with non-affiliated third parties, and for determining which exceptions (if any) cover those arrangements.

#### *(a) Arrangements with Service Providers and Joint Marketers*

Under this exception, PIM may share NPI with non-affiliated third parties that perform services for PIM. Examples of arrangements that fit within this exception are our arrangements with our auditors, outside legal counsel, and the brokers who execute trades for our client accounts.

The services contemplated by this exception include, but are not limited to, marketing of PIM's own products and services or those offered pursuant to a joint marketing agreement (i.e., a written contract under which PIM and one or more non-affiliated third parties jointly offer, endorse or sponsor a financial product or service). Examples of third-party marketers include marketing and advisory consultant, market research firms, and third-party solicitors or client referral sources. Also covered by this exception are arrangements with distributors of our products.

If PIM shares NPI with non-affiliated third parties pursuant to this exception, it does not need to provide an Opt-Out Notice to its Consumers and Customers, as long as it: (i) provides an initial Privacy Notice to its Customers (and, if required, its Consumers); and (ii) enters into a contractual agreement with the third party that prohibits the third party from disclosing or using the information other than to carry out the purposes for which PIM disclosed the information in the ordinary course of business.

The CCO shall be informed of any contracts with non-affiliated Service Providers and joint marketers with which PIM does business. Any PIM contracts with non-affiliated third parties must contain the appropriate confidentiality language.

***(b) Sharing Information as Necessary to Effect, Administer, Process or Enforce a Transaction that a Consumer or Customer Requests or Authorizes***

PIM may share NPI with non-affiliated third parties as necessary to process, service or administer a transaction that a Consumer or Customer requests or authorizes. It is under this exception, for example, that PIM could share NPI with a broker-dealer who executes trades for our client accounts. If PIM shares NPI with a non-affiliated third party under this exception, it is exempted from having to provide an Opt-Out Notice to its Customers and Consumers.

**(c)** ***Other Exceptions***

PIM is also exempted from having to provide an Opt-Out Notice to Customers and Consumers if it shares NPI:

(i) With the consent or at the direction of the Consumer, provided that the Consumer has not revoked the consent or direction;

(ii) To protect the confidentiality or security of records pertaining to the Consumer, service, product, or transaction;

(iii) To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

(iv) For required institutional risk control or for resolving Consumer disputes or inquiries;

(v) To persons holding a legal or beneficial interest relating to the Consumer;

(vi) To persons acting in a fiduciary or representative capacity on behalf of the Consumer;

(vii) To provide information to insurance rate advisory organizations, guaranty funds or agencies, agencies that rate PIM, persons that are assessing compliance with industry standards, and PIM's attorneys, accountants, and auditors;

(viii) To the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies, to self-regulatory organizations, or for an investigation on a matter related to public safety;

(ix) In connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of information concerns solely Consumers or Customers of such business or unit;

(x) To comply with federal, State, or local laws, rules and other requirements;

(xi) To comply with a properly authorized civil, criminal or regulatory investigation, or subpoena or summons by federal, State or local authorities; or

(xii) To respond to judicial process or government regulatory authorities having jurisdiction over PIM for examination, compliance, or other purposes as authorized by law.

### 2. Limits on Redisclosure and Reuse of Information Supplied by a Non-affiliated Third Party

The Regulation also limits our ability to share information about a non-affiliated third party's Consumers or Customers that we may obtain in the course of business. The rules vary depending on whether we receive the information for a Customer authorized transaction (section B.1.b.) or other exception (section B.1.c.) described above, or outside of those exceptions:

#### (a) Information We Receive Under an Exception

If we receive NPI for a Customer authorized transaction (section B.1.b.) or other exception (section B.1.c.) described above, we are limited in our ability to disclose the NPI to: (i) affiliates of the non-affiliated third party from which we received the NPI; (ii) our affiliates that are bound by our same limits to use the NPI; and (iii) use of NPI in the ordinary course of business to carry out activities pursuant to such exceptions. This applies to NPI we receive from brokers, administrators and anyone else with whom we enter into a service contract which involves the sharing of NPI.

#### (b) Information We Receive Outside of an Exception

If we receive NPI outside of a Customer authorized transaction (section B.1.b.) or other exception (section B.1.c.) described above, we are limited in our ability to disclose the NPI to: (i) affiliates of the non-affiliated third party from which we received the NPI; (ii) our affiliates that are bound by our same limits to use the NPI; and (iii) any other person, if the disclosure would be lawful if made directly to that person by the non-affiliated third party from which we received the information.

The CCO is responsible for enforcing this requirement with respect to PIM's employees. Employees violating these policies will be subject to appropriate disciplinary action.

### 3. Limits on Sharing Account Number Information for Marketing Purposes

The Regulation generally prohibits us from disclosing account numbers, or similar forms of access numbers or codes, for transaction accounts to non-affiliated third parties for use in telemarketing, direct mail marketing or other marketing through electronic mail. The prohibition, however, does not apply for disclosures to: (i) agents or Service Providers solely in order to perform marketing for our products and services, as long as the agent or Service Provider is not authorized to directly initiate charges to the account; and (ii) participants in a private label credit card program or an affinity or similar program where the participants in the program are identified to the Customer when entering into the program.

## C. Safeguarding Customer Information

PIM has adopted the following procedures that address administrative, technical, and physical safeguards for the protection of Customer records and information. For purposes of these safeguards, all of PIM's clients shall be considered Customers. These procedures are designed to: (i) ensure the security and confidentiality of Customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of Customer records and information; and (iii) protect against unauthorized access to or use of Customer records or information that could result in substantial harm or inconvenience

to any Customer. These procedures are further supplemented by our *Information Technology & Cybersecurity Policy*, and other privacy obligations and procedures in our *Data Protection Policy*, *Privacy Procedure*, and our *Data Protection Impact Assessment Procedure*.

1. PIM maintains a secure physical environment with building access limited to approved personnel and their supervised guests. Building entry and office access require ID cards that are assigned to employees and allow them access to the premises during their term of employment. ID cards are assigned and revoked via a controlled process managed by the Human Resource department using a Personal Action Form ("PAF Form"). Access to sensitive areas such as our server room are further restricted via specific authorization of the CIO.
2. All client files containing NPI shall be maintained at PIM's principal business office for the duration of the client relationship and for a minimum of two years thereafter. PIM endeavors to limit the use of paper files that contain client NPI, preferring to maintain such information in secure PIM computer systems and technology platforms. However, as some sensitive client information may still be retained in paper form, PIM maintains locked drawers to secure such materials. Non-essential client-related files (e.g., monthly custodian/bank statements) which are greater than two years old may be sent to an offsite storage facility which has agreed in writing to a reasonable confidentiality provision in its agreement with PIM.
3. PIM generally permissions computer system file level access based on the duties of specific departments, and leverages the PAF Form to manage the application access levels appropriate for individual employees. However, many files remain more broadly accessible to personnel across departments. To ensure computer terminals remain secure, all computers are locked when inactive and protected with complex passwords and multi-factor authentication.
4. PIM utilizes firewalls and other security detection software as deemed appropriate by the CCO, the CIO and MIS after consultation with PIM's outside management information systems consultant. PIM utilizes software security tools to manage the security of personal devices and to encrypt sensitive data.
5. Many client files and reports containing client information are contained within the systems provided to PIM by third party vendors. Access to these systems is password protected and is limited to personnel who need to know such information as part of their normal and authorized client servicing functions.
6. All databases containing names, addresses, contact and product information of clients shall be accessible by all PIM personnel as part of their normal and authorized client servicing functions. However, only certain persons whose duties require them to be able to do so shall have the ability to change the information in such files.
7. PIM personnel shall be instructed and periodically reminded to use extra caution in external email correspondence and to limit, to the extent practical or feasible, the use of full client names and/or the combination of client names with account numbers. Dates of birth and social security numbers or tax id numbers should not be transmitted by email without the approval of the CCO. Personnel should also remember that cell phones are not as secure as landlines and should try to avoid communicating non-public client information over cell phones, except in emergencies when cell phone service is the only alternative available.
8. Upon the opening of an account, the client will be assigned an alpha or alpha numeric short name which will be used on all reports, and by which the client will be referred whenever possible

in internal oral and written communications. Employees are reminded not to discuss client identities with unauthorized persons, including family members.

**9.** PIM's standard form investment advisory contracts will contain a confidentiality provision under which PIM will represent to hold all client information in confidence, subject to law and PIM's policies. This includes all aspects of the client's account, including holdings, performance, client identities and even the status of the account, with such obligations continuing after account closure. Employees cannot and should not send performance, transaction and other client account related information to anyone, including the client's consultants, attorneys, and accountants, unless the client has given email, fax or other written authorization to send such information. Authorizations are kept in the client's file, which should be checked any time a new or unfamiliar request for information is received.

**10.** No client name will be used on any representative client list unless and until the client has given prior written consent to the use of his/her name. Employees are reminded that all inquiries regarding clients should be directed to the CCO or President. No employee should respond to press or other inquiries regarding clients, even if they are asked to simply confirm a client identity.

**11.** Client references, even if they are relatives or friends, should not be provided without express approval of the CCO. There are multiple reasons for this: (i) the permission given by PIM's clients for use of their name does not extend beyond use in the representative client list PIM gives to prospects and consultants; (ii) federal law imposes conditions on the use of testimonials, and any piece that directly or indirectly contains a client's endorsement or describes a client's experience with the adviser may be deemed to be a testimonial; and (iii) any piece that includes a selective list of clients would have to contain various disclaimers and disclosures.

**12.** PIM's employees may share NPI collected from its clients within the company, including among its affiliates, and may disclose such information to other non-affiliated financial services companies (such as custodians and brokers or dealers) as part of the ordinary course of providing financial products and services to PIM's clients, for the purpose of offering new products and services to PIM's clients, for product development purposes, and as otherwise required or permitted by law. PIM's employees also may share this information with PIM's legal representatives, such as outside legal counsel, accountants and auditors, and with any governmental authorities, rating agencies, industry organizations and other applicable regulatory or administrative bodies.

**13.** Disclosures of composite or model portfolio holdings must be in accordance with PIM's *Advertising & Marketing Policy*, which generally provides that such disclosures must be limited to what is already public knowledge (i.e., holdings information in PIM's 13F filings or in an already distributed quarterly newsletter). The *Advertising & Marketing Policy* also permits holdings information to be disclosed to a prospective client as part of their due diligence or to a new client as part of their transition to PIM as their new portfolio manager so long as such disclosures are accompanied by confidentiality disclaimers, agreements and/or acknowledgements.

**14.** In addition to PIM's requirements regarding non-disclosure of client portfolio holdings, mutual fund clients and other clients may have their own policies regarding dissemination of portfolio information. Copies of such policies, if any, will be distributed periodically by the Compliance department and should be read and abided by as if fully incorporated into PIM's policies. Additional copies of such policies will be kept in the respective client's investment guidelines drawer on our record retention system.

## D. Disposal of Customer Information

PIM will use reasonable measures to protect against unauthorized access to or use of information during Disposal of Customer Information. We note that the Regulation is not intended to require PIM to (i) maintain or destroy any record pertaining to an individual that is not imposed under other law; or (ii) alter or affect any requirement imposed under any other provision of law to maintain or destroy records.

1. Destruction of any Customer Information physically retained will be conducted in a responsible manner with sensitivity to the confidential nature of such material. Such materials will be shredded to ensure confidentiality is protected, and any Service Providers involved in the destruction process will be bound by appropriate contractual obligations.
2. PIM maintains controls over its computer and technology infrastructure, which includes responsible deletion of data and destruction of hardware (e.g., computer, copy machines, faxes, printers) to ensure hard drives are sanitized when removed from the organization, as further detailed in its *Information Technology & Cybersecurity Policy* and its *Decommissioning Procedures*.

## E. Incident Response Plan

PIM maintains written policies and procedures for an incident response program that is reasonably designed to detect, respond to, and recover from unauthorized access to or use of Customer Information. Under our *Cybersecurity Incident Response Plan*, PIM requires notice of breaches of Sensitive Customer Information in accordance with the Regulation. Our plan includes: (i) procedures to assess the nature and scope of any incident, including identifying the Customer Information Systems and types of Customer Information that may have been accessed or used without authorization; (ii) appropriate steps to contain and control the incident to prevent further unauthorized access or use; and (iii) procedures to notify affected individuals.

## F. Incident Notification

PIM will provide notification to affected individuals whose Sensitive Customer Information was, or is reasonably likely to have been, accessed or used without authorization. To identify affected individuals, we will conduct reasonable investigations to determine the facts and circumstances of any incident of unauthorized access to or use of Sensitive Customer Information, to reasonably determine whether such information has been, or is reasonably likely to be, used in a manner that would result in substantial harm or inconvenience to a Customer. In accordance with the Regulation, any notices we provide will be clear and conspicuous and provided by a means designed to ensure that each affected individual can reasonably be expected to receive it. We will provide this notice as soon as reasonably practicable, but not later than 30 days, after we become aware that unauthorized access to or use of Customer Information has, or is reasonably likely to have, occurred. We note, however, that in certain instances notice may be delayed under the Regulation if the SEC receives a written request from the Attorney General that such notice poses a substantial risk to national security or public safety.

## G. Service Provider Oversight

PIM requires oversight of applicable Service Providers, including prompt notice of privacy issues consistent with the Regulation. PIM maintains a *Best Execution Policy* for selection and oversight of brokers/dealers and a *Vendor Management Policy* that includes the establishment, maintenance, and enforcement of written policies and procedures reasonably designed to require oversight, including through due diligence and monitoring, of Service Providers. PIM also maintains a Best Execution Committee to oversee broker relationships and a Vendor Management Committee to ensure responsible onboarding, ongoing monitoring, and manage termination of Service Providers.

1. During the onboarding process, the Vendor Management Committee evaluates Service Provider access to NPI as part of a vendor criticality assessment, which informs the level of diligence and monitoring required by PIM.
2. Service Provider due diligence responses that are viewed by the Vendor Management Committee as higher risk will be discussed as necessary with the department head responsible for vendor selection, senior members of the Information Technology department, and/or representatives of our Risk or Operating Committees.
3. PIM obligates applicable Service Providers to take appropriate measures to: (i) protect against unauthorized access to or use of customer information; and (ii) provide notification as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred resulting in unauthorized access to a CIS maintained by the Service Provider. In addition to confidentiality and safeguarding representations, when onboarding Service Providers with access to customer information, PIM Legal will ensure we obtain written notice provisions consistent with the Regulation via contract, service level agreement, or other written representation. Upon receipt of Service Provider notification, PIM is required to promptly initiate its incident response program.
4. While PIM is permitted under the Regulations to enter into a written agreement with a Service Provider to notify affected individuals on its behalf, PIM generally prefers to manage such notifications directly. PIM recognizes that the obligation to ensure that affected individuals are notified in accordance with the Regulation is ultimately PIM's responsibility.

## H. Recordkeeping

PIM's *Record Retention Policy* requires it to maintain all records required for investment advisers under 17 CFR 275.204-2, including subsection a.25 which mandates maintenance of records covering safeguarding of customer information and incident response plans. Accordingly, PIM will maintain books and records to evidence its compliance with the requirements, including written documentation of: (i) policies and procedures to address administrative, technical, and physical safeguards for the protection of Customer Information and compliance with the Regulation; (ii) any detected unauthorized access to or use of Customer Information, as well as any response to, and recovery from such unauthorized access to or use of Customer Information; (iii) any investigation and determination made regarding whether notification is required pursuant to the Regulation, including the basis for any determination made, any written documentation from the United States Attorney General related to a delay in notice, as well as a copy of any notice transmitted following such determination; (iv) any policies and procedures to oversee, monitor, and conduct due diligence on Service Providers, including to ensure that we are notified when a breach in security has occurred at the Service Provider; (v) any contract or agreement entered into between PIM and a Service Provider; and (vi) policies and procedures to address the proper Disposal of Consumer and Customer Information.

PZENA Investment Management

**<u>Exhibit A</u> –– Form of PIM Privacy Notice**

**<u>PRIVACY POLICY NOTICE</u>**

This Privacy Policy Notice describes the Privacy Policy of Pzena Investment Management, LLC. Our ability to provide you with superior products and services and to maintain our client relationship with you depends on the personal financial information we collect from you. We value your business and are committed to maintaining your trust. That is why we have made your privacy a top priority. By explaining our Privacy Policy to you, we trust that you will better understand how we keep our client information private and secure while using it to serve you better. In this Notice, the terms "we," "our" and "us" refer to Pzena Investment Management, LLC ("PIM"), and its affiliates including Pzena Financial Services, LLC, employees and agents who need to know the information to enable us to provide our services to you. The term "you" in this Notice refers broadly to all of our individual clients (including prospective and former individual clients).

**The Privacy Policy Notice explains the following:**

1) How we protect the confidentiality of our clients' non-public information
2) Who is covered by our Privacy Policy
3) The types of information we have about you and where it comes from
4) When, why and with whom we share client information

**Protecting the Confidentiality of Client Information**

We take our responsibility to protect the privacy and confidentiality of client information very seriously. We maintain physical, electronic and procedural safeguards including the use of firewalls, password protection and security detection software devices, to store and secure information about you from unauthorized access, alteration and destruction. We have implemented an incident response plan to detect, respond to, and recover from any unauthorized access to client information. From time to time, we may enter into agreements with non-affiliated companies to provide services to us or make products and services available to you. Under these agreements, the companies may receive information about you, but they must safeguard this information and they may not use it for any other purposes. We maintain oversight of service providers with access to our client information and require notification of any unauthorized access to ensure you remain informed of any privacy issues.

**Who is Covered by the Privacy Policy**

We provide our Privacy Policy Notice to individual clients when they open a new account, and if we change our policies or practices regarding the sharing of your information. If we change our privacy policies to permit us to share additional information we have about you, or to permit disclosures to additional types of parties, you will be notified in advance, and, if required by law, you will be given the opportunity to opt out of such additional disclosure and to direct us not to share your information with such parties.

Our Privacy Policy applies to individuals who are clients or former clients of PIM. Similarly, prospective individual clients who receive information about or from PIM are covered by the Privacy Policy. Individuals who receive information about or from PIM through our website, www.pzena.com, also are covered by our privacy policy, posted on our website.

**Information We Have About You**

We collect and maintain a variety of personal information about you from a variety of sources, including:

1) Information we receive from you on our New Account Form and other forms, such as your name, address and phone number, your social security number; and your assets, income, and other household information;

2) Information we receive and maintain about your account with us, such as your account balances, transactions history, and your additions to or withdrawals from such account; and

3) Information we receive about you from financial advisors or consultants or other financial institutions whom you have authorized to provide such information to us.

**Information PIM Shares**

We do not disclose client information we collect as described above except as may be required or permitted by law.

We may share all of the client information we collect among ourselves and may disclose such information to other non-affiliated financial services companies (such as custodians and brokers or dealers) as part of the ordinary course of providing financial products and services to you, for product development purposes, and as otherwise required or permitted by law.

We also may share this information with our legal representatives, such as our counsel, accountants and auditors, and with any governmental authorities, rating agencies, industry organizations and other applicable regulatory or administrative bodies.

We may include client names on a representative client list, but only after the client has specifically consented in writing to such inclusion. We may also share client information with persons with whom you specifically direct or authorize us to share such information, such as your accountant, financial consultant or attorney.

Finally, we may share client information with non-affiliated parties in connection with the performance of services for us, such as investor relations, marketing or mailing services, or in connection with joint marketing agreements we may have with other financial institutions.

**On all occasions when it is necessary for us to share your personal information with non-affiliated companies, such information may only be used for the limited purpose for which it is shared and we do not allow these companies to further share your information with others except to fulfill that limited purpose.**