Premier Investment Management, LLC

Registered Investment Advisor

PRIVACY POLICY V-22-02

Premier Investment Management, LLC
1481 Meadow Bluff Lane
Draper, UT 84020
(385) 259-3568
www.MyPimConnect.com

Table of Contents

Information Collected and Shared

PIM's privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed with client consent once annually if the policy is updated. The CCO will document the date the privacy policy was delivered to each client for each year if an annual delivery is required. PIM may collect information about clients from the following sources:

1. Information received from client on applications, via other forms, or during conversations;
2. Information about client's transactions with PIM or others; and
3. Information provided by a consumer reporting agency.

Proper Dissemination of Client Information

Below are the reasons for which PIM may share a client's personal information:

1. With specific third parties as requested by the client (see Sample 11);
2. For everyday business purposes – such as to process client transactions, maintain client account(s), respond to court orders and legal investigations, or report to credit bureaus;
3. For marketing by PIM – to offer PIM's products and services to clients;
4. For joint marketing with other financial companies;
5. For affiliates' everyday business purposes – information about client transactions and experience;
6. For non-affiliates to market to clients (only where allowed).

If a client decides to close his or her account(s) or becomes an inactive customer, PIM will adhere to the privacy policies and practices as described in this manual, as updated.

Storing Client Information

PIM uses various methods to store and archive client files and other information. Third party services or contractors used have been made aware of the importance PIM places on both firm and client information security. PIM also restricts access to clients' personal and account information to those employees who need to know that information to provide products or services to its clients. In addition to electronic protection, procedural safeguards, and personnel measures, PIM has implemented reasonable physical security measures at its home office location.

In addition, IT persons or other technical consultants employed at the firm may also have access to non-public client information at any time. An onsite or offsite server that stores client information, third party software that generates statements or performance reports, or third party client portals designed to store client files all hold the potential for a breach of non-public client information.

To mitigate a breach of client information, PIM uses encryption software on all computers and carefully evaluates any third party providers, employees, and consultants with regard to their security protocols, privacy policies, and/or security and privacy training.

Identity Theft Red Flags

The CFTC (U.S. Commodity Futures Trading Commission), SEC (U.S. Securities and Exchange Commission), and many state regulators, have published rules concerning identity theft encouraging or requiring

investment advisers to train firm personnel to recognize "red flags" regarding identity theft of advisory clients.

SAFEGUARDING IDENTIFYING INFORMATION

The list below is information that all PIM personnel should monitor and safeguard to guard against any breach of a client's identity:

1. Individual client's social security numbers
2. Corporate or other entity client's tax identification numbers
3. Individual driver's license number or other personal identification card
4. Passport numbers
5. Financial account numbers (credit card, bank, investment, etc.) and any accompanying passwords or access codes

POTENTIAL CAUSES OF IDENTITY INFORMATION BREACHES

1. Loss of theft of computers and/or other equipment
2. Hacking of computer networks
3. Inadvertent exposure of client information to unauthorized individuals (non-locked files, files left on desk, cleaning services, shredding services, etc.)
4. Physical break ins / theft

PIM personnel are instructed to notify the Firm if they detect or have reason to believe that any of the above shown red flag activities may have occurred or if any of the red flag information listed may have been stolen or leaked by any firm personnel. The Firm's Executive are tasked with investigating the report and taking appropriate actions.

Staff Training

On an annual basis, PIM will conduct a firmwide training session to ensure that staff members are trained and equipped to implement the above policies regarding client privacy. New Employees will receive training, led by the Firm's Executives, within one (1) month of their initial hire date.

Client Records

Client records will be retained by PIM for at least 5 years after the year in which the record was produced, or as otherwise required by law. With respect to disposal of non-public personal information, PIM will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.

PIM takes the privacy and confidentiality of all its clients and personnel very seriously. It will continue to make, and document, any changes needed to promote the security of client information.