RWM

Retirement Wealth Management, LLC

Privacy Policy

Retirement Wealth Management, LLC ("RWM") has adopted various procedures to implement the firm's policy and reviews to monitor and ensure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

Non-Disclosure of Client Information

RWM maintains safeguards to comply with federal and state standards to guard each client's nonpublic personal information. RWM does not share any nonpublic personal information with any nonaffiliated third parties, except in the following circumstances:

1. As necessary to provide the service that the client has requested or authorized, or to maintain and service the client's account;

2. As required by regulatory authorities or law enforcement officials who have jurisdiction over RWM, or as otherwise required by any applicable law; and

3. To the extent reasonably necessary to prevent fraud and unauthorized transactions.

Employees are prohibited, either during or after termination of their employment, from disclosing nonpublic personal information to any person or entity outside RWM including family members, except under the circumstances described above. An employee is permitted to disclose nonpublic personal information only to such other employees who need to have access to such information to deliver our services to the client.

Safeguarding and Disposal of Client Information

RWM restricts access to nonpublic personal information to those employees who need to know such information to provide services to our clients.

Any employee who is authorized to have access to nonpublic personal information is required to keep such information in a secure compartments or receptacle on a daily basis as of the close of business each day. All electronic or computer files containing such information shall be password secured and firewall protected from access by unauthorized persons. Any conversations involving non public personal information, if appropriate at all, must be conducted by employees in private, and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations.

Safeguarding standards encompass all aspects of the RWM that affect security. This includes not just computer security standards but also such areas as physical security and personnel procedures. Examples of important safeguarding standards that RWM may adopt include:

1. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means (e.g. requiring employee use of user ID numbers and passwords, etc.);
2. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals (e.g. intruder detection devices, use of fire and burglar resistant storage devices);
3. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
4. Procedures designed to ensure that ensure that customer information system modifications are consistent with the firm's information security program(e.g. independent approval and periodic audits of system modifications);
5. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems (e.g. data should be auditable for detection of loss and accidental and intentional manipulation);
6. Response programs that specify actions to be taken when the firm suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies;
7. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures (e.g. use of fire resistant storage facilities and vaults; backup and store off site key data to ensure proper recovery); and
8. Information systems security should incorporate system audits and monitoring, security of physical facilities and personnel, the use of commercial or in-house services (such as networking services), and contingency planning. Any employee who is authorized to possess "consumer report information" for a business purpose is required to take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. There are several components to establishing 'reasonable' measures that are appropriate for the firm:
9. Assessing the sensitivity of the consumer report information we collect;
10. The nature of our advisory services and the size of our operation;
11. Evaluating the costs and benefits of different disposal methods; and
12. Researching relevant technological changes and capabilities.
    a. Some methods of disposal to ensure that the information cannot practicably be read or reconstructed that RWM may adopt include:
13. Procedures requiring the burning, pulverizing, or shredding or papers containing consumer report information;
14. Procedures to ensure the destruction or erasure of electronic media; and

15. After due diligence, contracting with a service provider engaged in the business of record destruction, to provide such services in a manner consistent with the disposal rule.

Privacy Notices

RWM will provide each natural person client with initial notice of the firm's current policy when the client relationship is established. RWM shall also provide each such client with a new notice of the firm's current privacy policies at least annually. If RWM shares nonpublic personal information relating to a non-California consumer with an nonaffiliated company under circumstances not covered by an exception under Regulation S-P, the firm will deliver to each affected consumer an opportunity to opt out of such information sharing. If RWM shares nonpublic personal information relating to a California consumer with a non affiliated company under circumstances not covered by an exception under SB1, the firm will deliver to each affected consumer an opportunity to opt in regarding such information sharing. If, at any time, RWM adopts material changes to its privacy policies, the firm shall provide each such client with a revised notice reflecting the new privacy policies. The Compliance Officer is responsible for ensuring that required notices are distributed to the RWM consumers and customers.