
McClain Value Management, LLC
IA Policies and Procedures Manual
7/24/2008 to Current

Privacy

Policy

As a registered investment adviser, McClain Value Management, LLC must comply with SEC Regulation S-P (or other applicable regulations), which requires registered advisers to adopt policies and procedures to protect the "nonpublic personal information" of natural person consumers and customers and to disclose to such persons policies and procedures for protecting that information. Nonpublic personal information includes nonpublic "personally identifiable financial information" plus any list, description or grouping of customers that is derived from nonpublic personally identifiable financial information. Such information may include personal financial and account information, information relating to services performed for or transactions entered into on behalf of clients, advice provided by McClain Value Management, LLC to clients, and data or analyses derived from such nonpublic personal information. McClain Value Management, LLC must also comply with the California Financial Information Privacy Act (SB1) if the firm does business with California consumers.

Background

The purpose of these privacy policies and procedures is to provide administrative, technical and physical safeguards which assist employees in maintaining the confidentiality of nonpublic personal information collected from the consumers and customers of an investment adviser. All nonpublic information, whether relating to an adviser's current or former clients, is subject to these privacy policies and procedures. Any doubts about the confidentiality of client information must be resolved in favor of confidentiality.

Responsibility

Phillip McClain is responsible for reviewing, maintaining and enforcing these policies and procedures to ensure meeting McClain Value Management, LLC's client privacy goals and objectives while at a minimum ensuring compliance with applicable federal and state laws and regulations. Phillip McClain may recommend any disciplinary or other action as appropriate. Phillip McClain is also responsible for distributing these policies and procedures to employees and conducting appropriate employee training to ensure employee adherence to these policies and procedures.

Procedure

McClain Value Management, LLC has adopted various procedures to implement the firm's policy and reviews to monitor and insure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

Non-Disclosure of Client Information

McClain Value Management, LLC Adviser takes steps to safeguard and treat as confidential the information of its clients, including Client. Adviser limits access to a client's personal and account information to those employees who need to know that information to provide investment advice to clients. Adviser educates all employees about the importance of confidentiality, client's privacy and safeguarding information. Adviser maintains physical, electronic, and procedural safeguards that comply with federal standards to protect client information. Adviser may disclose nonpublic personal information about clients to third parties to assist Adviser in servicing a client's account, to government entities in response to subpoenas, or to comply with federal, state and local laws, rules and other applicable legal requirements. Other than that, during the term of this Agreement and afterwards, Adviser will not disclose any nonpublic personal information about clients to any other third parties. Adviser reserves the right to change any of the policies described above, at any time. If Adviser changes its policy or practice, Adviser will provide Client with a revised privacy policy as required by law. Employees are prohibited, either during or after termination of their employment, from disclosing nonpublic personal information to any person or entity outside McClain Value Management, LLC, 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

McClain Value Management, LLC 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 authorized persons overhearing or intercepting such conversations.

Safeguarding standards encompass all aspects of the McClain Value Management, LLC 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 McClain Value Management, LLC may adopt include:

- 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.);
- 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);
- Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
- Procedures designed to 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);
- Where practical, dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information (e.g. require data entry to be reviewed for accuracy by personnel not involved in its preparation; adjustments and correction of master records should be reviewed and approved by personnel other than those approving routine transactions, etc.);
- 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);
- 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;
- 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
- 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:

- Assessing the sensitivity of the consumer report information we collect;
- The nature of our advisory services and the size of our operation;
- Evaluating the costs and benefits of different disposal methods; and
- Researching relevant technological changes and capabilities.

Some methods of disposal to ensure that the information cannot practicably be read or reconstructed that McClain Value Management, LLC may adopt include:

- Procedures requiring the burning, pulverizing, or shredding of papers containing consumer report information;
- Procedures to ensure the destruction or erasure of electronic media; and
- 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

McClain Value Management, LLC will provide each natural person client with initial notice of the firm's current policy when the client relationship is established. McClain Value Management, LLC shall also provide each such client with a new notice of the firm's current privacy policies at least annually. If McClain Value Management, LLC shares nonpublic personal information relating to a non-California consumer with a 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 McClain Value Management, LLC 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, McClain Value Management, LLC 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 McClain Value Management, LLC's consumers and customers.