BATES Financial Advisors, Inc.

Privacy and Information Safeguarding

Privacy and Information Safeguarding Index

Introduction

Privacy and Information Safeguarding Content

Introduction

Our firm has taken appropriate steps to implement a comprehensive information security program that is tailored to our information retention system and the needs of our customers, which includes administrative, technical and physical safeguards appropriate to the size and complexity of our firm and the nature and scope of our activities. Our firm's information security program is designed to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

To meet the goals of our firm's information security policies, underlying standards and procedures should be developed. The policies may be changed over time as business processes and technology changes. The security standards should be based upon accepted security practices and have been tailored for our firm's business practices.

General Information Security Standards

Security standards encompass all aspects of the organization that affect security. This includes not just computer security standards but also such areas as physical security and personnel procedures. Examples of important security standards 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);
- 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 our firm's information security program (e.g., independent approval and periodic audits of system modifications);
- 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);
- 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 our firm suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
- 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).
- 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.

Physical Security Standards

Examples of Physical Security Standards include:

- Client information shall not be left unattended in offices or conferences rooms unless these areas are secure.
- As a general practice, client files, documents, or other records shall be stored in locked cabinets or desks when not in use and, in all cases, secured at the end of the business day.
- Visitors shall not be allowed to walk unescorted in areas where client information is accessible.
- As a general practice, records or documents containing client information shall be destroyed or shredded before disposal.
- The security policies and procedures of off-site record storage facilities shall be periodically assessed.
- Protocols shall be established for "locking down" offices at the close of business and for access to offices after business hours.
- The effectiveness of physical access controls in each area, during both normal business hours and other times, shall be reviewed on a periodic basis.

Electronic Records Security Standards

Examples of Electronic Records Security Standards include:

- PCs with access to client information shall not, as a general practice, be left unattended, or in the alternative, screen savers/sleep mode should incorporate password protection.
- Password protections for access to network PCs, client network accounts, and e-mail user accounts should be implemented and passwords shall be changed periodically. Users should be trained to avoid easy-to-guess passwords, not to divulge their passwords, and not to store passwords where others can access them.
- An appropriate schedule to back up electronic files shall be implemented. Backup copies shall be tested to ensure that they are usable and should be stored securely. Security measures shall be implemented to prevent unauthorized access to backup copies.
- Our firm's network shall monitor and log access to files containing client information. Access to client information on our firm's network shall be limited to those employees who require such access to service the client or conduct firm operations.
- Processes shall be developed for (1) requesting, establishing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.
- The need for the use of encryption technology shall be considered in the event that our firm elects to communicate client information electronically.
- Our firm shall assess whether it collects nonpublic personal information from persons visiting its website through log in or such devices as "cookies" and establish appropriate policies for such information.
- Our firm shall review and assess security measures designed to prevent unauthorized access to client information residing on our firm's website.

Contingency and Disaster Security Standards

Examples of Contingency and Disaster Security Standards include:

- Our firm shall identify and communicate the mission- or business-critical functions that protect client information and resources that support critical functions.
- Physical and environmental controls should anticipate contingencies or disasters and the development of scenarios should be employed to develop appropriate response plans to a wide range of potential events.

Employee Security Standards

Examples of Employee Security Standards include:

- Employees shall be required to sign appropriate confidentiality agreements as part of their employment agreements.
- Our firm shall limit access to client information to those employees that require access to the information to either provide client services or conduct firm operations.
- Employees shall be prohibited from disclosing client information over the telephone or in response to an e-mail unless they have identified the person to whom they are communicating as either the client, a fiduciary representative of the client, or a party that needs the information to complete a transaction for the client (e.g., clearing brokers or custodians).
- Employees shall confirm the identity of persons requesting client information over the telephone or by e-mail by requiring personal identifying information, such as mother's maiden name or social security number, before releasing information (unless prior contact has created a relationship causing the employee to recognize the client's voice, etc.).
- Our firm shall develop contingency plans for dealing with both "friendly" and "unfriendly" terminations to ensure that access to client information is discontinued as soon as possible. This should include removal of access privileges, computer accounts, control of keys, and return of firm property. Terminated employees shall receive a briefing on continuing responsibilities for confidentiality and privacy of client information.

Risk Assessment

George E. Bates is the Privacy Officer and is responsible for taking reasonable and prudent measures to: (1) identify foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of client information or client information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of client information; and (3) assess the sufficiency of policies, procedures, client information systems, and other arrangements in place to control risks and, when deficiencies are detected, make the appropriate recommendations to management in order to correct such deficiencies.

Training

All employees should be trained to implement the firm's information security program. Employees should be trained to recognize, respond to and report unauthorized attempts to obtain information to the appropriate Privacy Officer.

Employees and new hires shall be provided with copies of the firm's information security policies.

Testing

Our firm's information program may be tested periodically by an internal auditor to ensure controls, systems and procedures are operating properly. Testing of the information security program should be adjusted in light of changes in technology, the sensitivity of customer information and internal and external threats to information security.

We will monitor, evaluate and adjust, as appropriate, our information security program in light of any relevant changes in technology, the sensitivity of our customer information, internal or external threats to information, and our own changing business arrangements, such as outsourcing arrangements and changes to customer information systems.

Service Provider Arrangements

With respect to third parties with which our firm shares client information or which have access to such information, we should adopt procedures to:

- Exercise appropriate due diligence in selecting our service providers and make inquiry as to their security policies and procedures;
- Require, when feasible, our service providers by contract to implement appropriate measures designed to meet the objectives of our firm's information security policies; and
- Where indicated by our firm's risk assessment, monitor service providers to confirm that they have not shared or reused client information in violation of privacy rules.