Burgess Chambers & Associates, Inc.

Privacy Policy Notice

Policy
As a registered investment adviser, BCA 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 BCA to clients, and data or analyses derived from such nonpublic personal information. BCA 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
The Chief Compliance Officer is responsible for reviewing, maintaining and enforcing these policies and procedures to ensure meeting BCA's client privacy goals and objectives while at a minimum ensuring compliance with applicable federal and state laws and regulations. The Chief Compliance Officer may recommend to the President any disciplinary or other action as appropriate. The Chief Compliance Officer is also responsible for distributing these policies and procedures to advisory professionals and staff members and conducting appropriate training to ensure adherence to these policies and procedures.

Procedure
BCA 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:

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

- As necessary to provide the service that the client has requested or authorized, or to maintain and service the client's account;
- As required by regulatory authorities or law enforcement officials who have jurisdiction over BCA, or as otherwise required by any applicable law; and
- To the extent reasonably necessary to prevent fraud and unauthorized transactions.

Advisory Professionals and staff members are prohibited, either during or after termination of their relationship with BCA, from disclosing nonpublic personal information to any person or entity outside BCA, including family members, except under the circumstances described above. An advisory professional or staff member is permitted to disclose nonpublic personal information only to such other advisory professionals or staff members who need to have access to such information to deliver our services to the client.

Safeguarding and Disposal of Client Information
BCA restricts access to nonpublic personal information to those advisory professionals and staff members who need to know such information to provide services to our clients.

Any advisory professional or staff member who is authorized to have access to nonpublic personal information is required to keep such information in a secure compartment 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 advisory professional or staff member in private, and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations.

Safeguarding standards encompass all aspects of BCA 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 BCA may adopt include:

- Access controls on client information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent advisory professionals and staff members from providing client information to unauthorized individuals who may seek to obtain this information through fraudulent means (e.g. requiring advisory professional and staff member use of user ID numbers and passwords, etc.);
- Access restrictions at physical locations containing client 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 client 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);
- Dual control procedures, segregation of duties, and advisory professional and staff member background checks for advisory professionals and staff members with responsibilities for or access to client 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 client 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 client information systems, including appropriate reports to regulatory and law enforcement agencies;
- Measures to protect against destruction, loss, or damage of client 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 advisory professional or staff member who is authorized to possess "client 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 client 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 BCA may adopt include:

- Procedures requiring the burning, pulverizing, or shredding or papers containing client 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
BCA will provide each client with initial notice of the firm's current policy when the client relationship is established.