ANTONELLI FINANCIAL ADVISORS

Investment Management & Comprehensive Wealth Planning

PRIVACY POLICY

As a registered investment adviser, Antonelli Financial Advisors, LLC must comply with the Privacy Rule of the Gramm-Leach-Bliley Act (GLB Act) as administered and enforced by the Federal Trade Commission, which requires state registered advisers to adopt policies and procedures to protect the "non-public personal information" of natural person consumers and customers and to disclose to such persons policies and procedures for protecting that information.

Antonelli Financial Advisors, LLC has adopted various procedures to implement the firm's policy and conducts 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

Antonelli Financial Advisors, LLC maintains safeguards to comply with federal and state standards to guard each client's non-public personal information ("NPI"). Antonelli Financial Advisors, LLC does not share any NPI 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 Antonelli Financial Advisors, LLC, or as otherwise required by any applicable law;
- to the extent reasonably necessary to protect the confidentiality or security of the financial institution's records against fraud and for institutional risk control purposes; and
- to provide information to the firm's attorneys, accountants and auditors or others determining compliance with industry standards.

Employees are prohibited, either during or after termination of their employment, from disclosing NPI to any person or entity outside Antonelli Financial Advisors, LLC, including family members, except under the circumstances described above. An employee is permitted to disclose NPI 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

Antonelli Financial Advisors, LLC restricts access to NPI to those employees who need to know such information to provide services to our clients.

Any employee who is authorized to have access to NPI is required to keep such information in a secure compartments or receptacle annually. All electronic or computer files containing such information shall be password secured and firewall protected from access by unauthorized persons. Any conversations involving NPI, 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 Antonelli Financial Advisors, 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 Antonelli Financial Advisors, 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);
- 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 Antonelli Financial Advisors, LLC may adopt include:

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

Initial Privacy Notice Delivery

- Antonelli Financial Advisors, LLC will provide each natural person client with initial notice of the firm's current privacy policy when the client relationship is established.
- If Antonelli Financial Advisors, LLC shares non-public personal information ("NPI") 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 Antonelli Financial Advisors, LLC shares NPI relating to a California consumer with a nonaffiliated 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