Policy

As a registered investment adviser, Keller Financial Group, Inc. must comply with SEC Regulation S-P, which requires 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.

Further, and as a SEC registered advisory firm, our firm must comply with SEC Regulation S-AM, to the extent that the firm has affiliated entities with which it may share and use consumer information received from affiliates.

Currently, all 50 states have data breach laws which require private entities or government agencies to notify individuals who have been impacted by security breaches that may compromise their personally identifiable information ("PII"). Keller Financial Group, Inc. will follow industry and business best practices when it comes to notifying our clients on data breaches, and will also periodically review our state's requirements.

Background

Regulation S-P / Privacy Rule

The purpose of these regulatory requirements and privacy policies and procedures is to provide administrative, technical and physical safeguards which assist employees in maintaining the confidentiality of non-public personal information ("NPI") collected from the consumers and customers of an investment adviser. All NPI, 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.

For these purposes, NPI includes non-public "personally identifiable financial information" plus any list, description or grouping of customers that is derived from non-public 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 the firm to clients, and data or analyses derived from such NPI.

Regulation S-P implements the GLB Act's requirements with respect to privacy of consumer nonpublic personal information for registered investment advisers, investment companies, and broker-dealers (each, a "financial institution"). Among other provisions, financial institutions are required to provide an ***initial*** notice to each customer that sets forth the financial institution's policies and practices with respect to the collection, disclosure and protection of customers' nonpublic personal information to both affiliated and nonaffiliated third parties. Thereafter, as long as the customer relationship continues to exist, the financial institution is required to provide an annual privacy disclosure to its customers describing the financial institution's privacy policies and practices unless it meets the requirements for the annual delivery exception as set forth below.

Significantly, on December 4, 2015, the President signed the *Fixing America's Surface Transportation Act* (the "FAST Act") into law. Among other provisions, the FAST Act includes an amendment of the consumer privacy provisions within the GLB Act. The amendment, which went into effect immediately, now provides an exception to the ***annual*** privacy notice distribution requirement if the financial

institution meets the following two criteria: (i) the financial institution does not share nonpublic personal information with nonaffiliated third parties (other than as permitted under certain enumerated exceptions) and (ii) the financial institution's policies and practices regarding disclosure of nonpublic personal information have not changed since the last distribution of its policies and practices to its customers.

Regulation S-AM

SEC Regulation S-AM, effective September 10, 2009, with a postponed compliance date from January 1, 2010 to June 1, 2010, requires SEC investment advisers, and other SEC regulated entities, to the extent relevant, to implement limitations on the firm's use of certain consumer information received from an affiliated entity to solicit that consumer for marketing purposes. Regulation S-AM provides for notice and opt-out procedures, among other things. The compliance date was extended to allow registered firms to establish systems to meet the new regulatory requirements.

Responsibility

Dwayne Keller is responsible for reviewing, maintaining and enforcing these policies and procedures to ensure meeting Keller Financial Group, Inc. client privacy goals and objectives while at a minimum ensuring compliance with applicable federal and state laws and regulations. Dwayne Keller may recommend to the firm's principal(s) any disciplinary or other action as appropriate. Dwayne Keller 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

Keller Financial Group, Inc. 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

- Keller Financial Group, Inc. maintains safeguards to comply with federal and state standards to guard each client's non-public personal information ("NPI"). Keller Financial Group, Inc. 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 Keller Financial Group, Inc., or as otherwise required by any applicable law;
- 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 Keller Financial Group, Inc., 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

Keller Financial Group, Inc. 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 compartment or receptacle. 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 Keller Financial Group, Inc. 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 Keller Financial Group, Inc. 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;
- ensuring measures are put in place for the ability to access client information from any third-parties, including CRM systems, in order to review, delete, or perform security assessments, as necessary;
- 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 Keller Financial Group, Inc. 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

- Keller Financial Group, Inc. will provide each natural person client with initial notice of the firm's current policy when the client relationship is established. Keller Financial Group, Inc. shall also provide each such client with a new notice of the firm's current privacy policies at least 30 days of update.
- If Keller Financial Group, Inc. 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 Keller Financial Group, Inc. 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 sharing.

Annual Privacy Notice Delivery

- If Keller Financial Group, Inc. 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 30 days of update deliver to each affected consumer an opportunity to ***opt out*** of such information sharing.

- If Keller Financial Group, Inc. shares NPI relating to a California consumer with a nonaffiliated company under circumstances not covered by an exception under SB1, the firm will 30 days of update deliver to each affected consumer an opportunity to ***opt in*** regarding such information sharing.

Annual Privacy Notice Exception

Keller Financial Group, Inc. will not have to deliver an annual privacy notice provided it (1) only shares NPI with nonaffiliated third-parties in a manner that does not require an opt-out right be provided to customers (e.g., if the institution discloses NPI to a service provider or for fraud detection and prevention purposes) and (2) has not changed its policies and practices with respect to disclosing NPI since it last provided a privacy notice to its customers.

If, at any time, Keller Financial Group, Inc. 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 Keller Financial Group, Inc. consumers and customers.

Data Breaches and Compromise of PII

Keller Financial Group, Inc. will follow industry and business best practices when it comes to notifying our clients on data breaches, including:

- Immediate written notification to the client and appropriate state governmental agencies within 45 days of the breach;
- When a data security incident involves a client's Social Security number, driver's license number, or state identification card number, our firm is required (state requirements may vary) to provide an offer for a complimentary credit monitoring for at least 18 months; and
- Keller Financial Group, Inc. will provide instructions to affected clients on how to sign up for complimentary credit monitoring services and will not require impacted clients to waive their private right of action as a condition of the offer of such services.