COVE STREET CAPITAL

STATEMENT OF PRIVACY PRINCIPLES FOR CONSUMER CUSTOMERS

SEPTEMBER 2014

Ms. Daniele Beasley | President & Chief Compliance Officer | dbeasley@covestreetcapital.com | t 424.221.5897

2101 East El Segundo Boulevard | Suite 302 | El Segundo, CA 90245 | www.CoveStreetCapital.com

POLICY

As a registered investment adviser, CSC 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.

In addition, our Firm's policy, to the extent applicable, is to comply with the FTC's FACT Act / Red Flags Rule which requires covered entities to develop and maintain an effective client identity theft prevention program.

Further, and as a SEC registered advisory firm, our firm must comply with new 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.

CSC must also comply with the California Financial Information Privacy Act (SB1) if the Firm does business with California consumers.

BACKGROUND

Regulation S-P

The purpose of these Reg S-P 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 Reg S-P purposes, NPI 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 CSC to clients, and data or analyses derived from such NPI.

Red Flags Rule

The Federal Trade Commission's ("FTC") FACT Act / Red Flags Rule, which became effective 1/1/2008, covers "financial institutions" and "creditors." The Rule defines "financial institution" as any state or federal bank or any person that directly or indirectly holds a "transaction account" belonging to a consumer. A "creditor" includes a broad category of businesses or organizations that regularly defer payment for goods or services which are billed later. The FTC has clarified that any person that provides a product or service for which the consumer pays after delivery is a creditor under the Red Flags Rule. Accordingly, an adviser who bills for advisory services in arrears is deemed to be a creditor and is, therefore, a "covered entity" under the Red Flags Rule. The FACT Act / Red Flags Rule requires covered entities to develop and maintain written identity theft prevention programs.

In October 2009, the FTC, at the request of Congress, extended for the fourth time the Fact Act/Red Flags Rule compliance date, from 1/1/2010 to 6/1/2010. Once again, the FTC announced that it has further delayed the compliance date for implementation of the Red Flags Rule pursuant to the request of

"Members of Congress," while Congress considers legislation that would affect the scope of the entities covered by the Rule. Accordingly, the revised compliance date is now December 31, 2010. Consistent with prior compliance date delays, the FTC indicated that the postponement is limited to the Rule. The deferment of the compliance date does not affect other federal agencies ongoing enforcement of corresponding identity theft program regulations.

On December 9, 2010, Congress sent the President the "Red Flag Program Clarification Act of 2010," excluding certain providers that deliver service before payment. On December 18, President Obama signed the bill into law. The legislation amends the Fair Credit Reporting Act (which the FACTA amended, and which states the penalties under the Red Flag rules) to redefine the term "creditor." Because the definition now includes one who uses or reports to consumer reporting agencies in connection with its transactions, and excludes one who "advances funds...for expenses incidental to a service provided by the creditor to that person," the definition is narrower and excludes many professionals, including most investment advisers.

Effective July 21, 2011, authority for the Red Flags Rule was transferred from the FTC to the SEC for firms over which the SEC has enforcement jurisdiction. While this change in authority has no immediate impact, the SEC has stated that at some future date it intends to conduct rulemaking that will set forth how the Red Flags Rule may apply to the SEC-registered investment advisers and other firms subject to its enforcement authority.

Regulation S-AM

New SEC Regulation S-AM, effective 9/10/2009, with a postponed compliance date from 1/1/2010 to 6/1/2010, 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

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

CSC 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

CSC maintains safeguards to comply with federal and state standards to guard each client's nonpublic personal information ("NPI"). CSC 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 CSC, or as otherwise required by any applicable law; and
- To the extent reasonably necessary to prevent fraud and unauthorized transactions.

Employees are prohibited, either during or after termination of their employment, from disclosing NPI to any person or entity outside CSC, 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

CSC 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 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 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 CSC 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 CSC 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 CSC 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 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

CSC will provide each natural person client with initial notice of the Firm's current policy when the client relationship is established. CSC shall also provide each such client with a new notice of the Firm's current privacy policies at least annually. This annual noticed is sent with the client's first quarter portfolio statement. If CSC shares nonpublic 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 CSC shares NP 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, CSC 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 CSC's consumers and customers.