11/19/2013 to Current

Privacy

Policy

As a registered investment adviser, Mitchell Vaught and Taylor, Inc. Investment Advisors must comply with SEC Regulation S-P (*OR if state-registered:* with the Privacy Rule of the Gramm-Leach-Bliley Act (GLB) as administered and enforced by the Federal Trade Commission), 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 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.

Mitchell Vaught and Taylor, Inc. Investment Advisors must also comply with the California Financial Information Privacy Act (SB1) if the firm does business with California consumers.

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 Mitchell Vaught and Taylor, Inc. Investment Advisors to clients, and data or analyses derived from such NPI.

Identity Theft / Red Flags Rules

In January 2001 the Federal Trade Commission's ("FTC") FACT Act / Red Flags Rules (the "Red Flags Rules") became effective covering "financial institutions" and "creditors." The Red Flags Rules define "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 clarified that any person that provides a product or service for which the consumer pays after delivery is a creditor under the Red Flags Rules.

In response to financial industry concerns regarding the applicability of the rules to various segments of the financial markets, the FTC repeatedly extended the rule's compliance date. On December 9, 2010, Congress sent the President the "Red Flag Program Clarification Act of 2010," excluding certain providers that deliver service before payment; which President Obama signed into law on December 18, 2010. The legislation amended the Fair Credit Reporting Act 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 Rules was transferred from the FTC to (i) the SEC for firms over which the SEC has enforcement jurisdiction (*i.e.,* federally-registered investment advisers, broker-dealers, mutual funds) and (ii) the CFTC for entities subject to its regulation (i.e., futures commodity merchants, commodity trading advisers, and commodity pool operators). State-registered advisers remain subject to the FTC's Red Flags for Identity Theft rules.

The SEC and CFTC (together, the "Commissions") issued joint proposed rules and guidelines requiring entities that are subject to their respective jurisdictions to address risks of identity theft in 2012. The Commissions jointly adopted Regulation S-ID: Identity Theft Red Flags ("Identity Theft Rules") on April 10, 2013.

The Identity Theft Rules require each SEC and/or CFTC-regulated entity that meets the definition of a

"financial institution" or a "creditor" that offers a "covered account" (as those terms are defined under the Fair Credit Reporting Act) to develop and implement by November 20, 2013 a written identity theft prevention program(the "Program") designed to detect, prevent and mitigate identity theft in connection with certain existing accounts and the opening of new accounts.

Notably, the final rules require that a firm's board of directors, an appropriate committee of the board of directors, or if the firm does not have a board, a designated senior management employee (i) provide initial approval of the Program and (ii) maintain responsibility for the ongoing oversight, development, implementation, and administration of the Program.

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

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

Mitchell Vaught and Taylor, Inc. Investment Advisors 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

Mitchell Vaught and Taylor, Inc. Investment Advisors maintains safeguards to comply with federal and state standards to guard each client's non-public personal information ("NPI"). Mitchell Vaught and Taylor, Inc. Investment Advisors 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 Mitchell Vaught and Taylor, Inc. Investment Advisors, 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 Mitchell Vaught and Taylor, Inc. Investment Advisors, 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

Mitchell Vaught and Taylor, Inc. Investment Advisors 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 Mitchell Vaught and Taylor, Inc. Investment Advisors 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 Mitchell Vaught and Taylor, Inc. Investment Advisors 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 Mitchell Vaught and Taylor, Inc. Investment Advisors 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

Mitchell Vaught and Taylor, Inc. Investment Advisors will provide each natural person client with initial notice of the firm's current policy when the client relationship is established. Mitchell Vaught and Taylor, Inc. Investment Advisors shall also provide each such client with a new notice of the firm's current privacy policies at least annually. If Mitchell Vaught and Taylor, Inc. Investment Advisors 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 Mitchell Vaught and Taylor, Inc. Investment Advisors 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. If, at any time, Mitchell Vaught and Taylor, Inc. Investment Advisors 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 Mitchell Vaught and Taylor, Inc. Investment Advisors' consumers and customers.

Identity Theft / Red Flags Rules

As a 'financial institution' or 'creditor' that offers and maintains one or more 'covered accounts' Mitchell Vaught and Taylor, Inc. Investment Advisors is required to adopt a written identity theft prevention program. Mitchell Vaught and Taylor, Inc. Investment Advisors has adopted reasonable procedures to implement the firm's policy and conducts reviews to monitor and ensure the policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

- identify relevant patterns, practices, and specific activities that are "red flags" signaling possible identity theft and incorporate those red flags into the Program;
- detect the occurrence of red flags occurring with the Program;
- respond appropriately to any detected red flags to prevent and mitigate identity theft;
- quarterly reviews and, if necessary, update the Program to reflect changes in risks to customers and to the safety and soundness of the financial institution from identity theft; and
- provide appropriate staff training to effectively implement the Program.With respect to third parties with which Mitchell Vaught and Taylor, Inc. Investment Advisors shares client information or which have access to such information, Mitchell Vaught and Taylor, Inc. Investment Advisors' oversight procedures include:
- a review of the service provider's security policy and procedures, conducted as part of our firm's initial due diligence assessment;
- require, when feasible, the service provider by contract to implement appropriate measures designed to meet the objectives of Mitchell Vaught and Taylor, Inc. Investment Advisors' data security policies;
- require the service provider to promptly notify Mitchell Vaught and Taylor, Inc. Investment Advisors of any security incident it experiences, including incidents not resulting in the actual compromise of Mitchell Vaught and Taylor, Inc. Investment Advisors' data; and
- require the service provider to annually deliver certification of the effectiveness of its data security policy and procedures.