

## Safeguards Rule Supplement<sup>1</sup>

### Who Must Comply?

Financial institutions that are not regulated by the Securities and Exchange Commission (“SEC”), the Commodity Futures Trading Commission (“CFTC”), or the Federal Reserve must comply with the Safeguards Rule. As such, hedge fund managers that are neither registered with the SEC nor the CFTC or both are required to comply with the Safeguards Rule.<sup>2</sup>

All hedge fund managers regardless of registration status should be alert that a theme discussed in the recent SEC Hedge Fund Roundtable was the cultivation of a “compliance culture” within the hedge fund industry.<sup>3</sup> Also note recent government initiatives to formalize compliance and procedures pursuant to the various securities and futures regulations.<sup>4</sup> Furthermore, compliance with the USA PATRIOT Act will require you to collect identifying information which contains nonpublic personal information as part of your know your customer due diligence obligations that you will have to safeguard.<sup>5</sup> As such, in light of these developments, we recommend that all hedge fund managers regardless of registration status consider the Federal Trade Commission’s (the “FTC”) recommendation set forth below.

### What Am I Required to Do?

The FTC requires a written information security plan (the “ISP”) that describes your firm’s program to protect customer information. The ISP is to be tailored to your firm’s size, complexity, and operations. *Essentially, you are to review your current privacy program and then enhance the program in light of the FTC’s recommendations.*

---

<sup>1</sup> Supplement to THSH Memorandum “FTC Issues Safeguards Rule to Further Protect Customer Privacy” (August 2002).

<sup>2</sup> See Standards for Safeguarding Customer Information; final rule, 16 C.F.R. 314.

<sup>3</sup> SEC Hedge Fund Roundtable held on May 14-15, 2003.

<sup>4</sup> See Securities and Exchange Commission; Compliance Program of Investment Companies and Investment Advisers; proposed rules. 68 Fed. Reg. 7038-7050 (February 11, 2003). See also THSH Memorandum to Clients “SEC Proposed Rules: Compliance of Registered Investment Companies and Registered Investment Advisers” (March 2003) See NFA Notice to Members Notice 1-03-05. See also THSH Memorandum to Clients “National Futures Association Ethics Training and Disaster Recovery and Business Continuity Requirements” (May 22, 2003).

<sup>5</sup> See Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Unregistered Investment Companies; proposed rule. 67 Fed. Reg. at 60617-60625 (September 26, 2002). See e.g. Financial Crimes Enforcement Network; Securities and Exchange Commission; joint final rules. 68 Fed. Reg. 25131-25149. (May 9, 2003). It is expected that final rule to require hedge funds to adopt an anti-money laundering program pursuant to the USA PATRIOT Act will be issued. See Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Investment Advisers; proposed rules. 68 Fed. Reg. 23646-23653, note 19 (May 5, 2003); A Report to Congress in Accordance with Section 356(c) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorist Act of 2001 (USA PATRIOT Act) Submitted by the Secretary of the Treasury, the Board of Governors of the Federal Reserve System, the Securities and Exchange Commission (December 31, 2002).

The FTC has identified three critical areas you should concentrate: (1) employee management and training; (2) information systems; and (3) managing system failures.

## **I. Employee Management and Training**

The FTC recommends that you consider doing the following:

### A. Employees

- Check references prior to hiring employees who will have access to customer information; and
- Require employees to sign an agreement to follow your firm's confidentiality and security standards for handling customer information.

### B. Employee Training – issues to cover:

- Locking rooms and file cabinets where paper records are kept;
- Using password-activated screensavers;
- Using strong passwords (at least eight characters long);
- Referring calls or other requests for customer information to designated individuals who have had safeguards training; and
- Recognizing any fraudulent attempt to obtain customer information and reporting it to appropriate law enforcement agencies.

We also recommend that employees sign a certificate evidencing their participation in an employee training session each time such a session is conducted.

## **II. Information Systems**

According to the FTC, “information systems” include network and software design, and information processing, storage, transmission, retrieval, and disposal. The FTC recommends the following:

### A. Storage

- Store paper records in a room, cabinet, or other container that is locked when unattended;
- Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods;
- Store electronic customer information on a secure server that is accessible only with a password;
- Do not store sensitive customer data on a machine with an Internet connection; and
- Maintain secure backup media and keep archived data secure.

## B. Disposal

- Hire or designate a records retention manager to supervise the disposal of records containing nonpublic personal information;
- Shred or recycle customer information recorded on paper and store it in a secure area until a recycling service picks it up; and
- Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives or any other electronic media that contain customer information.

## **III. Managing System Failures**

According to the FTC, effective security management includes the prevention, detection and response to attacks, instructions or other system failures. Your firm's technology support staff should consider the following:

- Having a written contingency plan to address security breaches;
- Checking software vendors to obtain and install patches that resolve software vulnerabilities;
- Using anti-virus software that updates automatically;
- Maintaining up-to-date firewalls, particularly if you use broadband Internet access or allow employees to connect to your network from home or other offsite locations; and
- Take steps to preserve the security, confidentiality and integrity of customer information in the event of a computer or other technological failure such as backing up all customer data regularly.

\* \* \* \* \*

If you have any questions or comments regarding compliance with the Safeguards Rules or compliance with the privacy rules under to the Gramm-Leach Bliley Act, please feel free to contact:

Michael G. Tannenbaum  
(212) 508-6701  
tannenbaum@tanhelp.com

Ricardo W. Davidovich  
(212) 508-6710  
davidovich@tanhelp.com

Roderick J. Cruz  
(212) 702-3149  
cruz@tanhelp.com