

TANNENBAUM HELPERN SYRACUSE & HIRSCHTRITT LLP

MEMORANDUM

FTC Issues Safeguards Rule to Further Protect Customer Privacy¹

Under the Gramm-Leach-Bliley Act (“GLB Act”)², financial institutions that are located in the U.S. and are subject to the Federal Trade Commission’s (“FTC”) jurisdiction are required to undertake measures to protect the nonpublic personal information (“NPI”), (e.g. name, address, income, social security number)³ of customers (e.g. investors) who are U.S. and non-U.S. natural persons.⁴ As part of its implementation of the GLB Act, on May 17, 2002, the FTC issued final rules implementing Section 501(b) of the GLB Act (the “Safeguards Rule”).⁵ The purpose of the Safeguards Rule is to establish standards relating to administrative, technical and physical information safeguards as required by Section 501(b) of the GLB Act. Such standards are intended to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and to protect against unauthorized access to or use of such records on information that could result in substantial harm to a customer.

With respect to privacy, the FTC has jurisdiction over financial institutions that are not otherwise regulated by another U.S. federal regulatory body.⁶ As such, *operators of hedge funds that are not otherwise regulated by the Securities Exchange Commission*

¹ By Michael G. Tannenbaum, Esq. and Roderick J. Cruz, Esq. Michael G. Tannenbaum is a founding partner of Tannenbaum Helpers Syracuse & Hirschtritt LLP and is head of the law firm’s financial services, capital markets and derivatives practice group. Roderick J. Cruz is an associate in the financial services, capital markets and derivatives practice group. This memorandum provides general information on the subject matter described, and it should not be relied on for legal advice on any matter, which may turn on specific facts. You should seek specific legal advice before acting with regard to the subjects treated here.

² Pub. Law 106-102.

³ See “How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act, A Guide for Small Business from the Federal Trade Commission” (July 2002) available at <<http://www.ftc.gov/bcp/online/pubs/buspubs/glblong.htm>>.

⁴ See Privacy of Consumer Financial Information; final rule, 16 C.F.R. 313; “Frequently Asked Questions for the Privacy Regulations” (December 2001) available at <http://www.ftc.gov/privacy/glbact/glb_faq.htm>. “The privacy regulations apply to all United States offices of financial institutions that are subject to the FTC authority under the GLB Act, regardless of where the consumer lives.” See “Frequently Asked Questions for the Privacy Regulations” (December 2001) available at <http://www.ftc.gov/privacy/glbact/glb_faq.htm>.

⁵ See Standards for Safeguarding Customer Information; final rule, 16 C.F.R. 314; “FTC Issues Financial Information Safeguards Rule,” Press Release (May 17, 2002). See also Federal Trade Commission – Business Alert, “Safeguarding Customers’ Personal Information: A Requirement for Financial Institutions,” available at <<http://www.ftc.gov/bcp/online/pubs/alerts/safealrt.htm>>.

⁶ See 16 C.F.R. 313.1(6): “The ‘financial institutions’ subject to the [Federal Trade] Commission’s enforcement authority are the those that are not otherwise subject to the enforcement authority of another regulator under Section 505 of the Gramm-Leach-Bliley Act.”

and/or the Commodity Futures Trading Commission/National Futures Association will have to comply with the Safeguards Rule.

Pursuant to the Safeguards Rule, a financial institution must adopt a written information security program (“ISP”).⁷ With respect to its ISP, a financial institution must cover the following five elements:

1. Designate an employee or employees to coordinate the ISP;
2. Conduct risk assessment to identify internal and external risks to security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction of such information. Moreover, the FTC considers three areas to be the “most relevant” when conducting risk assessment: (i) employee training; (ii) information systems design, processing, storage, transmission and retrieval; and (iii) preventing, detecting and responding to attacks, intrusions or system failures;
3. Design an ISP and detail the plans to monitor the ISP;
4. Require third-party service providers that a financial institution has retained, by contract, to implement and maintain information safeguards; and
5. Evaluate and adjust the ISP in light of changes to a financial institution’s business operations or the results of its monitoring and security tests.⁸

A provision which will likely impact the hedge fund industry is the requirement that a financial institution ensure that its third-party service provider comply with the Safeguards Rule.⁹ In general, for most hedge funds, an administrator handles the subscription process which entails receiving, processing and accessing an investor’s personal and financial information. As such, the administrator is in the position of being a recipient of an investor’s NPI. Accordingly, pursuant to the Safeguards Rule, a financial institution must require its service provider, *by contract*, to implement and maintain information safeguards. Therefore, a hedge fund operator will have to review an administrator’s information operations and then negotiate and enter into a contract that obligates an administrator to adopt the same provisions under the Safeguards Rule. How administrators will react to this regulatory burden and whether administration fees will rise remain to be seen.

*Financial institutions must implement their ISPs by May 23, 2003.*¹⁰ As such, hedge fund operators have the next nine months to evaluate their operations and to develop an ISP. Furthermore, there is a transition rule for contracts entered into by June 23, 2002 between financial institutions and third-party service providers.¹¹ This transition rule gives

⁷ See 16 C.F.R. 314.3(a).

⁸ See 16 C.F.R. 314.4(a)-(e).

⁹ See 16 C.F.R. 314.4(d)(2).

¹⁰ See 16 C.F.R. 314.5(a). See also FTC Commentary to 16 C.F.R. 314. The Safeguards Rule will take effect one year from the date on which the final rule is published in the Federal Register which was May 23, 2002. See FTC Commentary to 16 C.F.R. 314.

¹¹ See 16 C.F.R. 314.5(b). See also FTC Commentary to 16 C.F.R. 314. Contracts between financial institutions and nonaffiliated third-party service providers are given two years to bring service provider

financial institutions two years to require its service providers, by contract, to implement an ISP.¹² Accordingly, *hedge fund operators have until May 23, 2004 to bring service contracts with administrators into compliance with the Safeguards Rule.* To assist financial institutions in complying with the Safeguards Rule, the FTC will issue guidance on how to implement and monitor an ISP and on how to oversee a third-party service provider in the near future.¹³

* * * * *

If you have any questions or comments regarding compliance with the Safeguards Rule, please feel free to contact Michael G. Tannenbaum at (212) 508-6701, Ricardo W. Davidovich at (212) 508-6710 or Roderick J. Cruz at (212) 702-3149.

August 2002

contracts into compliance with the Safeguards Rule as long as the contract was in place 30 days after the date on which the final rule was published in the Federal Register which was May 23, 2002. See FTC Commentary to 16 C.F.R. 314.

¹² See 16 C.F.R. 314.5(b). See also FTC Commentary to 16 C.F.R. 314.

¹³ See FTC Commentary to 16 C.F.R. 314.