

COMPLIANCE WITH NEW SAFEGUARDS RULE ADOPTED BY THE FEDERAL TRADE COMMISSION

As you may recall from our prior memos, all investment advisers and private investment fund operators not registered with the Securities and Exchange Commission (the “SEC”) or the Commodity Futures Trading Commission (the “CFTC”) (“Unregistered Advisers”) and private investment funds not subject to SEC or CFTC regulation (together with Unregistered Advisers, “Private Investment Fund Organizations”) are currently required to comply with the Federal Trade Commission’s (“FTC”) privacy rules (which took effect on May 24, 2000) (the “FTC Privacy Rules”) mandated by the Gramm-Leach-Bliley Act. The FTC Privacy Rules require, among other things, that Private Investment Fund Organizations maintain administrative, technical and physical safeguards to protect the security, integrity and confidentiality of customer records and information.

In furtherance of this requirement, on May 23, 2003, the FTC declared effective a new rule setting forth the standards for developing, implementing and maintaining such safeguards (the “Safeguards Rule”). The objectives of the Safeguards Rule are to: (1) ensure the security and confidentiality of customer information, (2) protect against any anticipated threats or hazards to the security or integrity of such information and (3) protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to any customer.

Under the Safeguards Rule, all financial institutions subject to the FTC’s jurisdiction (including Private Investment Fund Organizations) must have in place a comprehensive (written) information security program. Each information security program must be developed, implemented and maintained in accordance with the following criteria:

- one or more employees must be designated by each Private Investment Fund Organization to coordinate its information security program;
- such program must be designed to: (1) identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that may result in unauthorized disclosure, misuse, alteration, destruction or other compromise of such information and (2) assess the sufficiency of any safeguards currently in place to control these risks;¹

¹ At a minimum, such risk assessment should include consideration of risks in each relevant operational area, including: (1) employee training and management; (2) information systems (including network and software design, as well as information processing, storage, transmission and disposal); and (3) detecting, preventing and responding to attacks, intrusions or other systems failures.

- the program must have a mechanism for design and implementation of information safeguards to control risks identified through the above risk assessment and regularly test or otherwise monitor the effectiveness of the program;
- Private Investment Fund Organizations must oversee service providers by (1) taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the relevant customer information and (2) require their service providers (by contract) to implement and maintain such safeguards; and
- the program must be evaluated and modified periodically in response to certain material changes in risk assessment (e.g., due to changes in operations or business arrangements).

Although each information security program must include these basic elements, the Safeguards Rule allows Private Investment Fund Organizations to select specific safeguards that are appropriate to their size and complexity, the nature and scope of their activities and the sensitivity of the customer information they maintain.

To assist Private Investment Fund Organizations (as well as other entities subject to the FTC's jurisdiction) in complying with the Safeguards Rule, the FTC's staff will offer a brief training program concerning the Safeguards Rule's requirements. The training program will be offered on two alternative dates: June 9, from 10-11 a.m., and June 23, from 2-3 p.m. Both sessions will be held in Washington, DC, at 601 NJ Avenue NW, in the FTC Conference Center, Room A on the first floor. The sessions are open to the public and there is no advance registration. Interested parties who cannot attend in person are encouraged to participate by telephone; instructions on how to dial in will be posted on the FTC's Web site at www.ftc.gov one day in advance of each presentation.

Although the Safeguards Rule has taken effect, it nonetheless provides affected entities additional time to bring certain service provider contracts into compliance with the Safeguards Rule. More specifically, for any service provider contract entered into prior to June 24, 2002, the Safeguards Rule allows Private Investment Fund Organizations until May 24, 2004, to add appropriate contract provisions concerning safeguards.

* * * * *

If you have any questions concerning this memorandum or would like to receive copies of the FTC Privacy Rules or the Safeguard Rule, please call Daniel Schloendorn (212-728-8265), Niral Kalaria (212-728-8713) or Brendan R. Kalb (212-728-8166).

Willkie Farr & Gallagher is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our website is located at www.willkie.com.

June 4, 2003

Copyright © 2003 by Willkie Farr & Gallagher.

All Rights Reserved. This memorandum may not be reproduced or disseminated in any form without the express permission of Willkie Farr & Gallagher. This memorandum is provided for news and information purposes only and does not constitute legal advice or an invitation to an attorney-client relationship. While every effort has been made to ensure the accuracy of the information contained herein, Willkie Farr & Gallagher does not guarantee such accuracy and cannot be held liable for any errors in or any reliance upon this information.