WILLKIE FARR & GALLAGHER LLP

NEW YORK WASHINGTON HOUSTON PARIS LONDON FRANKFURT BRUSSELS MILAN ROME

CLIENT MEMORANDUM

NFA Proposes Cybersecurity Safeguards

September 16, 2015

AUTHORS

Rita M. Molesworth | **Deborah A. Tuchman** | **James E. Lippert** | **Marc J. Lederer**

In light of growing cybersecurity concerns, the National Futures Association recently submitted to the CFTC an interpretive notice on certain NFA supervisory rules. If approved by the CFTC, the Notice would require NFA members to adopt and enforce written procedures to secure customer data and access to a member's electronic systems ("information systems security programs" or "ISSPs").

NFA Rules 2-9, 2-36 and 2-49 require each futures commission merchant, commodity trading advisor, commodity pool operator, introducing broker, retail foreign exchange dealer, swap dealer and major swap participant to diligently supervise its business and risks attendant thereto. The Notice would serve to provide a general framework to design, implement and monitor security procedures so that NFA members may "diligently supervise the risks of unauthorized access to or attack of their information technology systems, and to respond appropriately should unauthorized access or attack occur."[1]

[1] National Futures Association: Information Systems Security Programs—Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49; Information Systems Security Programs (August 28, 2015), available here.

The Notice would not establish specific ISSP standards, as NFA recognizes that ISSPs will need to be tailored to fit the unique circumstances of each member. The Notice would require an ISSP to cover several key areas, which are comparable to the areas addressed in regulations and/or guidance issued by other regulators.[2] The Notice proposes to require that ISSPs be in writing and contain (i) a security and risk analysis, (ii) a description of the safeguards deployed against identified threats and vulnerabilities and (iii) a description of the process used to evaluate the nature of a detected security event, understand its potential impact and take appropriate measures to contain and mitigate the breach. ISSPs would also have to (i) describe the NFA member's internal education and training procedures related to information security and (ii) address the risks posed by critical third-party service providers.

An NFA member's ISSPs would have to be approved by the member's chief executive officer, chief technology officer or other executive-level officer. NFA would also expect senior management of the member to periodically provide information about the ISSP to the member's board of directors or similar governing body to enable it to monitor the information security efforts of the member.

To the extent that an NFA member is part of a larger holding company structure, the member would be able to meet its obligations through its participation in a consolidated entity ISSP. Nevertheless, the member would still be obligated to ensure that all written policies and procedures relating to the program (i) are appropriate to its information security risks, (ii) are maintained in a readable and accessible manner and (iii) can be produced upon request to NFA and the CFTC.

The Notice also proposes to require each NFA member to monitor and review, at least annually, the effectiveness of its ISSP, including the efficacy of the safeguards the member has deployed, and make adjustments as appropriate.

---

[2] Many NFA members may already have ISSPs in place as a result of compliance with other laws and regulations, such as the Gramm-Leach-Bliley Act, the Securities and Exchange Commission and CFTC's Identity Theft Red Flags Rules, the anti-money laundering rules, state data security laws and international data security rules. NFA noted that it reviewed guidance issued by the Financial Industry Regulatory Authority, the SEC, the Securities Industry and Financial Markets Association and the Department of Justice in developing the Notice. NFA also noted that the supervisory standards may overlap with rules and/or guidance of other financial regulators, as well as with other NFA rules. Thus, NFA believes that for many members the Notice simply builds upon existing custom. NFA recognizes, however, that smaller members may need additional, more detailed guidance and intends to initially work with members to assist them in developing their ISSPs. For more information on the SEC and CFTC's Identity Theft Red Flags Rules, please see our client memorandum entitled "SEC and CFTC Adopt Identity Theft Red Flag Rules," dated May 2, 2013.

If you have any questions regarding this memorandum, please contact Rita M. Molesworth (212-728-8727, rmolesworth@willkie.com), Deborah A. Tuchman (212-728-8491, dtuchman@willkie.com), James E. Lippert (212-728-8945, jlippert@willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com) or the Willkie attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Paris, London, Frankfurt, Brussels, Milan and Rome. The firm is headquartered at 787 Seventh Avenue, New York, NY 10019-6099. Our telephone number is (212) 728-8000 and our fax number is (212) 728-8111. Our website is located at www.willkie.com.

September 16, 2015