FUNKHOUSER VEGOSEN LIEBMAN & DUNN LTD.

Legal Update

February 2016

NFA MEMBERS MUST ADOPT INFORMATION SYSTEMS SECURITY PROGRAMS BY MARCH 1st

By William J. Bolotin and Cecilia M. Suh

If they have not already done so, National Futures Association (NFA) Members should review their current cybersecurity procedures and implement Information Systems Security Programs this month. The NFA's Interpretive Notice 9070, "NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs," requires NFA Members to adopt and enforce written policies and procedures (called ISSPs) to protect customer data and access to their electronic systems. The Interpretive Notice takes effect on March 1, 2016, and applies to all NFA membership categories, including futures commission merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers, and major swap participants.

Each Member should ensure that it has written policies and practices in place that are reasonably designed to: (1) diligently supervise the risks of unauthorized access to or attack of the Member's IT systems and (2) respond appropriately if an unauthorized access or attack occurs. The Interpretive Notice provides general requirements and guidance regarding the ISSPs that Member firms should adopt and tailor to their particular business activities and risks. More specifically, Members should ensure that their ISSPs include the following components:

1. Adoption and Enforcement of a Written ISSP

NFA Members are required to have a written policy that supports informed decision-making and escalation within the firm to identify and manage information security risks. The written ISSP should be reasonably designed to protect against security threats or hazards to the Member's technology systems, which are appropriate to the firm's size, complexity of operations, role in the financial industry, types of customers and counterparties, sensitivity of data accessible within its systems, and electronic interconnectivity with other entities.

2. A Security and Risk Analysis

A Member's written ISSP is also required to contain a security and risk analysis. Accordingly, Members should maintain an inventory of critical IT hardware with network connectivity, data transmission or data storage capability, and critical software. Members should also identify significant internal and external threats and vulnerabilities to at-risk data that is collected, maintained, and disseminated (including customer and counterparty personally identifying information, corporate records, and financial information); assess the threats to and the vulnerability of their electronic infrastructure; assess the threats posed through any applicable third-party service providers or software; and know the devices connected to their network and network structure.

The security and risk analysis should generally include risks such as loss, destruction, or theft of critical hardware containing at-risk data; viruses, spyware, and other malware; and interception and compromise of email.

FVLD®

© 2016, Funkhouser Vegosen Liebman & Dunn Ltd.
All rights reserved.

3. Description of Safeguards Against Identified Threats and Vulnerabilities

The ISSP should document and describe the protective measures the Member firm uses to protect against the identified threats and vulnerabilities. What safeguards are used will depend upon factors such as the Member's size, business, technology, electronic interconnectivity with other entities, and the potential threats identified in its security and risk analysis.

Members should also document and implement reasonable procedures to detect potential threats. These steps may include utilizing network monitoring software, monitoring the presence on the Member's physical premises of unauthorized users, or establishing procedures designed to identify unauthorized connections to the Member's network.

4. Incident Response Plan to Recover from Security Threats

The ISSP must include an incident response plan to manage detected security events or incidents, analyze the potential impact, and take appropriate measures to contain and mitigate the threat. The ISSP should contain procedures for restoring compromised systems and data and communicating with appropriate stakeholders and regulatory authorities.

5. Employee Education and Training

Each Member, considering its identified security risks and the composition of its workforce, must provide training regarding information security to all appropriate personnel upon hiring as well as periodically during their employment. The ISSP must contain a description of this training.

6. Annual Review

Members should regularly review the effectiveness of their ISSPs, including the safeguards deployed, and make adjustments as appropriate. Members are required to review their ISSPs at least once every 12 months.

7. Assessment of Risks Posed by Critical Third-Party Service Providers

The ISSP must address risks posed by critical third-party service providers. These may include providers that have access to a Member's systems, operate outsourced systems for the Member, or provide cloud-based services (*e.g.*, data storage or application software).

8. Recordkeeping Requirements

Finally, all records relating to a Member's adoption and implementation of an ISSP and that document a Member's compliance with the Interpretive Notice must be maintained pursuant to NFA Compliance Rule 2-10.

Conclusion

NFA Members must adopt and enforce written ISSPs tailored to each Member's business activities and specific risks in accordance with the Interpretive Notice. The NFA recognizes that there is no "one-size-fits all ISSP" and Members may need to rely on different resources and processes to develop appropriate ISSPs. Members should consult with counsel, as well as IT providers/departments, to review existing cybersecurity practices and implement ISSPs that are appropriate for their businesses.

FVLD publishes updates on legal issues and summaries of legal topics for its clients and friends. They are merely informational and do not constitute legal advice. We welcome comments or questions. If we can be of assistance, please call or write William J. Bolotin 312.701.6880 wbolotin@fvldlaw.com, Peter T. Berk 312.701.6870 pberk@fvldlaw.com, Cecilia M. Suh 312.701.6841 csuh@fvldlaw.com, or your regular FVLD contact.

FVLD®

© 2016, Funkhouser Vegosen Liebman & Dunn Ltd.
All rights reserved.