

CLIENT ALERT

NFA to Require Cyber Breach Reporting

December 14, 2018

AUTHORS

Rita M. Molesworth | Deborah A. Tuchman | James E. Lippert | Michael A. DeNiro

The National Futures Association has proposed an amendment to its existing interpretive guidance on information systems security programs that would, among other things, require NFA members to provide notice to NFA in the event of a cybersecurity breach that results in a loss of customer or counterparty funds or certain other enumerated consequences.¹ NFA members should expect to become subject to the new interpretive guidance in the near future.

NFA Interpretive Guidance on ISSPs

In 2016, NFA issued an interpretive notice (the “Notice”) that requires 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”).² The Notice provides 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 ... respond appropriately should unauthorized access or attack occur.”³ In recognition of the fact that members’

¹ See NFA: Proposed Amendments to NFA’s Interpretive Notice: *NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs* (Dec. 4, 2018), available [here](#).

² See NFA Interpretive Notice 9070, *NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs* (eff. Mar. 1, 2016).

³ *Id.* For additional information on the Notice, please see our client memorandum entitled “NFA Proposes Cybersecurity Safeguards,” dated September 16, 2015, available [here](#).

NFA to Require Cyber Breach Reporting

businesses differ in type, size and complexity of operations, the Notice provides a degree of flexibility to each member to design and implement security standards, procedures and practices that are appropriate to such member.⁴

Proposed Changes to the Notice

NFA is proposing to amend the Notice to incorporate a notification requirement relating to cybersecurity incidents and to provide clarification on certain other items relating to ISSP approval and training, as further described below.

Notification Requirement

The Notice currently requires a member's ISSP to include an incident response plan that addresses how the member will communicate internally and with external stakeholders, including customers, regulators and law enforcement, in the event of an information security incident. As amended, the Notice would also require members (other than certain FCMs for which NFA is not the DSRO) to promptly notify NFA in the event of an information security incident related to the member's commodity interest business that results in (i) any loss of customer or counterparty funds; (ii) any loss of the member's own capital; or (iii) the member providing notice to customers or counterparties under state or federal law (e.g., state data breach notification statutes). Members would be required to provide a written summary to NFA of the incident with the relevant details. If a member provides a notice to customers or counterparties, the member may provide a copy of such notice to NFA in lieu of a written summary.

As amended, the Notice would further encourage members to be familiar with any additional notice requirements to which they are subject under U.S. and non-U.S. data security and privacy laws and regulations and recommend that FCMs and introducing brokers consider filing suspicious activity reports with FinCEN, where appropriate, as part of reporting cyber incidents to regulators and agencies.

ISSP Approval

The Notice currently requires that a member's ISSP be approved by the member's chief executive officer, chief technology officer or other executive-level officer. NFA is proposing to amend the Notice to require that the ISSP be approved by the member's CEO or other senior level officer with primary responsibility for information security or by another senior official who is a listed principal of the member and has authority to supervise the execution of its ISSP. In the case of a member that participates in a consolidated entity ISSP that has been approved at the parent company level, the amended Notice would require that the member's CEO, chief technology officer, chief information security officer (or

⁴ We note that NFA members may have ISSPs (or their equivalent) in place to comply with other legal and regulatory obligations not directly related to their commodity interest activities. For example, NFA members that are also registered as investment advisers with the SEC would be expected to have policies and procedures in place based on requirements under applicable federal laws and regulations, guidance from the SEC and its staff and state law notification statutes. The Notice recognizes this and generally permits members to build upon existing procedures.

NFA to Require Cyber Breach Reporting

person with equivalent responsibility) or a senior official who is a listed principal of the member approve in writing that the ISSP's written policies and procedures are appropriate for the member's information security risks.

ISSP Training

Members are currently required to provide information security training to their employees at hiring and periodically thereafter. As amended, the Notice would require that members provide the periodic training no less frequently than annually (and more frequently if circumstances warrant). The amended Notice would also require that the description of a member's ongoing education and training in its ISSP identify the topics to be covered in the training.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

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

Michael A. DeNiro

212 728 8147

mdeniro@willkie.com

Copyright © 2018 Willkie Farr & Gallagher LLP.

This alert is provided by Willkie Farr & Gallagher LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This alert may be considered advertising under applicable state laws.

Willkie Farr & Gallagher LLP is an international law firm with offices in New York, Washington, Houston, Palo Alto, 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.