Client Update
NFA Cybersecurity Notice Takes Effect March 1

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Byungkwon Lim
blim@debevoise.com

Jim Pastore
jjpastor@debevoise.com

Gary E. Murphy
gemurphy@debevoise.com

Michael Decker
mdecker@debevoise.com

WASHINGTON, D.C.
Jeewon Kim Serrato
jkserrato@debevoise.com

The Cybersecurity Interpretive Notice, issued by the National Futures Association ("NFA") and approved by the Commodity Futures Trading Commission, becomes effective March 1, 2016. The Notice requires all Members of NFA (futures commission merchants, swap dealers, major swap participants, introducing brokers, forex dealer members, commodity pool operators and commodity trading advisors) to have in place practices that are reasonably designed to 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.

The March 1 deadline is not expected to trigger any immediate charges of noncompliance. Rather, it is expected that NFA will work with Members to help them move into a position of compliance. Members should expect compliance to be a topic in future examinations.

KEY INFORMATION SYSTEMS SECURITY PROGRAM CONSIDERATIONS

The full text of the Notice can be found here. Some highlights:

- The Notice focuses on five key areas for a Member's information systems security program ("ISSP"): a written program, security and risk analysis, deployment of protective measures against the identified threats and vulnerabilities, response and recovery from events that threaten the security of the electronic systems, and employee training.
- The Notice specifically singles out risks related to third-party service providers and provides guidance on risk management practices, such as performing due diligence on a third party's security practices and adding measures in contracts that address how confidential data will be protected and implementing procedures to respond to data breach notices from a service provider.

- Members will have a leg up if they have already been benchmarking their cybersecurity efforts against the standards of certain leading cybersecurity organizations. The Notice points favorably to a number of such standards as appropriate guideposts, including the Cybersecurity Framework issued by the National Institute for Standards and Technology and the Critical Security Controls for Effective Cyber Defense issued by the SANS Institute.
- Significant C-Suite and board-level engagement is required. The written ISSP should be approved in writing by the Member's Chief Executive Officer, Chief Technology Officer or other executive level official, and senior management should periodically update the Member's board of directors (or similar governing body or committee) with information about the ISSP that is sufficient for monitoring the Member's information security efforts.
- The Notice calls for eternal vigilance: Members are called on to perform a regular review of their ISSP at least annually, using either in-house staff with appropriate knowledge or engaging an independent third-party information security specialist.
- NFA recognizes that one size does not fit all. The Notice does not establish specific technology requirements, instead proposing guidelines that leave the exact form of an ISSP up to each Member in light of its particular circumstances.
- Where a Member is part of a larger corporate structure that shares common information systems and has adopted and implemented privacy and security safeguards organization-wide, the Member firm can satisfy the supervisory responsibilities described in the Notice through a consolidated entity ISSP.

NFA MEMBERS' "FAQ"

I Can't Possibly Meet All These Obligations by March 1. What to Do?

Keep calm and carry on. NFA has made clear that it will take a cooperative approach and not a punitive one. At a recent workshop, NFA said it will not simply start saying "violation, violation, violation" after March 1; rather, it will work with Members to help move them towards compliance. NFA recognizes that some Members will need to devote a significant amount of time and resources to meet their obligations and that any programs that are adopted will be refined over time.

The key for now is to get as far as you can by March 1, and to have a plan and timetable for the work that remains. All signs are that NFA realizes that good

cybersecurity solutions tend to take time, and tend to be effective only if implemented in an orderly manner.

Where Do I Start?

We suggest that Members that are part of larger institutional groups with ISSPs, or that otherwise have existing ISSPs in place or in development, start by reviewing any such ISSP for consistency with the Notice. Members can then make plans to identify and close any delta between their existing ISSPs and the requirements of the Notice. Firms that are starting closer to scratch are encouraged to look to the NIST Framework and to NIST's list of implementation resources.

Will I Be Hearing from NFA?

Likely yes. NFA intends to develop an incremental, risk-based examination approach regarding the Notice's requirements. NFA has not specified that cybersecurity will necessarily be a topic in your next examination, but it is prudent to assume that it will be.

Am I at Risk of Enforcement Action if My Cybersecurity Isn't up to Snuff?

History says eventually yes. NFA has explicitly attempted to model the Notice on the cybersecurity efforts of other bodies, like the SEC and FINRA, that have begun to bring enforcement actions. The gist of these cases is that although a regulated firm is the victim of outside hackers, it can still be deemed legally responsible for not keeping its guard up. It seems likely, though not imminent, that NFA and the CFTC may in time take a similar approach.

* * *

We are available to discuss any questions that our clients and friends may have about the Cybersecurity Interpretive Notice.