CFTC Approves NFA Interpretive Notice on Information Systems Security Programs, Including Cybersecurity Guidance

Written by Catherine M. Anderson, Kate Leonard

October 30, 2015

The CFTC recently approved the National Futures Association's interpretive notice (the "Cybersecurity Notice") on the general requirements that members should implement for their information systems security programs ("ISSPs"), which includes cybersecurity guidance and ongoing testing and training obligations.

The Cybersecurity Notice will be effective March 1, 2016 and applies to futures commissions merchants, commodity trading advisors, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers, and major swap participants (each, a "Member"). The Cybersecurity Notice emphasizes that the exact form of an ISSP should be adopted and tailored to the Member's size, complexity of operations, type of customers and counterparties, and its electronic interconnectivity with other entities; there is no one-size-fits-all ISSP. However, the ISSP must include the following:

Information Security Program

- *Written Program:* Members are required to implement a written ISSP program that is approved in writing by the individual Member's Chief Executive Officer, Chief Technology Officer, or other executive level official. Members may consider several resources for creating and appropriately tailoring a comprehensive ISSP, including the cybersecurity best practices and standards promulgated by the SANS Institute (SANS), the Open Web Application Security Project (OWASP), ISACA's Control Objectives for Information and Related Technology (COBIT), and the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).
- *Security Risk and Analysis:* Members are required to evaluate and prioritize their information technology system's risks, which includes the maintenance of an inventory of critical hardware and software systems. Also included in this risk analysis is the identification and assessment of the severity of the risks and major threats associated with the particular systems used and their protection of sensitive data. The report should also include details of past security incidents and known risks.
- *Deployment of Protective Measures:* Based upon the risk security and analysis, Members must memorialize and describe the steps taken to protect against identified weaknesses, as well as the procedures implemented to identify new threats. Members are given broad latitude to tailor these programs based on the individual Member's size, business, and the threats identified.
- *Incident Response and Recovery:* Members are required to create a plan in the event that one or more of its systems is compromised, including procedures to mitigate damage and plans to communicate the breaches externally, including providing notification to law enforcement and/or regulators.
- *Employee Training:* Members should include ongoing training and education for their employees, which should be administered at an employee's initial hire and periodically. The training should be tailored to the risks the Member faces.

ISSP Review

Members should review their ISSPs at least annually and should make regular adjustments as needed. Reviews may include penetration testing and/or third-party analyses customized to the Member's business.

Third-Party Service Providers

ISSPs should address the special risks that third-party service providers pose to the protection of sensitive data, which may include performing due diligence on providers of critical services to ensure that they have adequate security measures in place. Further, arrangements made with these third-party providers should address and describe the measures taken to protect sensitive data, including the restriction or removal of access to such data.

Recordkeeping

ISSPs, like Members' other records, must be maintained in accordance with NFA Compliance Rule 2-10.

The full text of the Cybersecurity Notice is **available here**. For further recent Foley Advisers on cybersecurity, please see: **SEC Charges Investment Adviser with Violating Regulation S-P by Failing to Adopt Cybersecurity Policies and Procedures**; **SEC Issues Risk Alert on Cybersecurity Initiative for Investment Advisers**; **SEC Office of Compliance Inspections and Examinations Releases Cybersecurity Examination Sweep Summary of Investment Advisers and Broker-Dealers**; and **OCIE's 2015 Cybersecurity Examination Initiative**.

RELATED INDUSTRIES

- Investment Advisers & Private Funds
- Professional Services

RELATED PRACTICES

- Business Counseling
