Securities
Regulation Daily

Wolters Kluwer

May 24, 2018

Increased Enforcement Activity Underscores Need for Firms to Conduct Rigorous Cybersecurity Oversight

By Kevin Angle, Paulita Pike, Elizabeth Reza and Heather Sussman
*Ropes & Gray, LLP**

Cybersecurity Oversight

Financial regulators continue to expand their reach in the cybersecurity space, and funds, fund sponsors, and advisers should take note. Most recently, on February 12, the CFTC filed a simultaneous Order and Settlement against AMP Global Clearing LLC (AMP), a registered futures commission merchant, related to a breach of its networks in April 2017 by a third party who obtained approximately 97,000 AMP files, including customers' personal information. Notably, the CFTC did not charge AMP under its regulation requiring that registrants have in place policies and procedures to safeguard customer records and infomation; rather, the CFTC proceeded under a separate regulation requiring that registrants diligently supervise any delegated entity tasked with performing any aspect of the registrant's business activities. The Order and Settlement highlight the importance for funds, fund sponsors, and advisers of adequately supervising their service providers' cybersecurity measures.

Background on the AMP Order and Settlement

AMP had adopted a written information systems security program (ISSP) that delegated to an IT provider the implementation of certain provisions, including (1) identifying and performing risk assessments of network access routes, and (2) performing quarterly network risk assessments to identify and report vulnerabilities to AMP. In June 2016, the IT provider installed a back-up data storage device, but failed to identify a default feature that allowed third parties to access AMP's backup files from the Internet without permissions. In April 2017, a third party detected this vulnerability on AMP's network and successfully copied approximately 97,000 files from the installed back-up data storage device, unbeknownst to AMP. The CFTC therefore concluded that the IT provider violated the ISSP, first by failing to identify or run a risk assessment of the problematic feature in its initial installation, and second by failing to report any network abnormalities or concerns in each of three quarterly network risk assessments between the time of installation and when the third party accessed the AMP network.

---

* This is the first article from a working group of investment management and cybersecurity attorneys at Ropes & Gray, LLP. We look forward to sharing more insights on cybersecurity trends and developments of concern to the investment management industry.

The CFTC proceeded, however, not against the service provider (which was outside of its jurisdiction, in any event), but against AMP for failure to supervise the vendor. As evidence of its failure to diligently supervise its IT provider, the CFTC pointed to the 10-month period during which AMP was unaware that thousands of customer records were unprotected, and the fact that AMP only learned of the subsequent breach when notified by the third party. Notably, the CFTC did not identify any specific action (or lack thereof) by AMP in determining that AMP had failed to adequately supervise its service provider, instead pointing to circumstantial factors such as the length of time the vulnerability remained unremediated as the bases for its charge.

CFTC and SEC Cybersecurity Regulations

Regulations and interpretive notices published by the CFTC and the National Futures Association (NFA), the self-regulatory organization for the U.S. derivatives industry, put in place a framework for registrants' obligations for cybersecurity. CFTC registered entities are required, for example, to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information" under Regulation 160.30. The CFTC has issued a staff advisory clarifying that the policies and procedures should be in writing and should identify reasonably foreseeable security risks and the controls for assessing and mitigating such risks. The NFA's Interpretive Notice 9070 similarly requires NFA Members to "adopt and enforce a written ISSP reasonably designed to provide safeguards appropriate to the Member's size, complexity of operations, type of customers and counterparties, the sensitivity of the data accessible within its systems, and its electronic interconnectivity with outer entities, to protect against security threats or hazards to their technology systems."

The SEC has issued similar rules, compliance with which will also satisfy obligations under CFTC Regulation 160.30. Regulation S-P requires registered broker-dealers, investment companies, and investment advisers to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." The regulation goes further to specify that policies and procedures must be "reasonably designed" to protect customer information, protect against anticipated threats to the security of customer information, and prevent any unauthorized "access to or use of" any customer information that could result in "substantial harm or inconvenience to any customer."

Interestingly, however, in its recent action against AMP, the CFTC did not rely on Regulation 160.30 and related notices. Instead, the CFTC brought charges under Regulation 166.3, which broadly imposes supervisory obligations on CFTC-registered fund sponsors and commodity trading advisers. In doing so, the CFTC expanded its enforcement reach beyond failures to maintain policies and procedures to the supervisory obligations of registrants in the cybersecurity space. AMP had adopted an ISSP pursuant to NFA Interpretive Notice 9070—but its cybersecurity obligations did not end there.

Duty to Supervise

Both the CFTC and SEC have in place regulations imposing supervisory obligations on registered fund sponsors and commodity trading advisers, and registered investment companies, advisers, and

broker-dealers, respectively. CFTC registrants, for example, are required to "diligently supervise the handling by its partners, officers, employees and agents" of all of the registrant's business activities, including the securing of networks handling such business. Identifying a violation of the operative regulation, Regulation 166.3, is a fact-intensive determination that examines whether (1) the registrant's supervisory system is generally inadequate, or (2) the registrant failed to perform is supervisory duties diligently. Registrants have an affirmative duty to actively supervise their delegates by instituting procedures for both detecting and preventing wrongdoing by such persons, including appropriate supervisory structures and compliance programs. Evidence of inadequate supervision can come from the nature of the violations themselves or from repeated violations.

Under the fund compliance rule (Rule 38a-l), the SEC similarly requires every registered investment company and business development company to "[a]dopt and implement written policies and procedures reasonably designed to prevent violation of the Federal Securities Laws by the fund, including policies and procedures that provide for the oversight of compliance by each investment adviser, principal underwriter; administrator, and transfer agent of the fund." Rule 206(4)-7 likewise requires advisers to institute policies and procedures to prevent violations, which could include oversight of their vendors' cybersecurity. Indeed, oversight of vendors has been cited by the SEC's Division of Investment Management as a key measure for implementing effective compliance programs under Rules 38a-1 and 206(4)-7. In guidance published by the SEC's Office of Compliance Inspection and Examination (OCIE) on its Cybersecurity Examination Initiative, which reviewed the cybersecurity practices of broker-dealers, investment advisers, and investment companies, OCIE has also stressed the importance of implementing practices and controls related to vendor management, including ongoing monitoring and oversight of vendors. OCIE has gone as far as to indicate that an element of robust policies and procedures is to require third-party vendors to periodically provide logs of their activities on a firm's network.

In the AMP Order, the CFTC connects registrants' information security obligations with their diligent supervision obligations—asserting that it "flow[s] naturally" from a registrant's obligation to adopt appropriate policies and procedures to safeguard customer information under Regulation 160.30 that the same registrant must, under Regulation 166.3, diligently supervise how those policies and procedures are implemented by downstream service providers, including the IT providers tasked with securing a registrant's network infrastructure and customer data. With the AMP Order, the CFTC is sending a clear signal that registrants cannot "abdicate" their data security responsibilities under Regulation 166.3 by simply passing them on to a service provider without further liability.

The AMP action emphasizes the importance of robust cybersecurity oversight of vendors and the ease with which a regulated entity can find itself in the crosshairs of an enforcement action. The broader regulatory landscape and the SEC's toolbox can lead to similar results. Comprehensive, documented technical and physical safeguards for customer records and information alone are not sufficient. Funds, fund sponsors, and advisers should also actively oversee the cybersecurity activities of their vendors and document those efforts. The level of diligence required, which could include security questionnaires or more detailed examinations, could depend on the level of access granted to the vendor as well as an overall assessment of the vendor's risk profile. For vendors providing critical IT services, such as with AMP, a more rigorous level of oversight is likely required.