Davis Polk

Delegation, Not Abdication: The CFTC Fines AMP Global Clearing LLC for Failing to Supervise a Third-Party Service Provider

February 21, 2018 | Client Update | 4-minute read

For the first time, the CFTC has fined a company for poor cybersecurity practices that resulted in a third-party breach of the company's information systems. This development is consistent with an increasing trend of regulators holding companies responsible for the cybersecurity failures of third-party service providers.

AMP Global Clearing LLC ("**AMP**") was fined $100,000 by the CFTC on February 12, 2018 for failing to diligently supervise its information technology provider's implementation of certain provisions of AMP's information systems security program ("**ISSP**"). The CFTC's **order** states that from June 21, 2016 to April 17, 2017, AMP's customers' records and information were left unprotected and were eventually compromised by an unaffiliated third party. AMP's lack of awareness of its vulnerability to cyber exploitation and the resulting breach is, according to the CFTC, evidence of its failure to diligently supervise its information technology provider ("**IT Provider**"), as required under **CFTC Regulation 166.3**.

The Regulatory Background. Under **CFTC Regulation 160.30**, futures commission merchants ("**FCMs**") are required to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." An FCM may delegate the performance of its ISSP but must "diligently supervise the handling [of its ISSP] by its partners, officers, employees and agents." Whether an FCM meets its regulatory obligation is a "fact-intensive determination." As described below, in an action that appears to be the first of its kind, the CFTC found that the compromise of AMP's data served as factual evidence of AMP's failure to comply with Regulation 166.3.

AMP's Facts. AMP delegated to its IT Provider certain provisions of its ISSP, including requirements to:

- Identify and perform risk assessments of access routes into AMP's network;
- Perform quarterly risk assessments to identify vulnerabilities and report those results to AMP's officers;
- Maintain strict firewall rules to ensure access to AMP's network only from known IP addresses; and
- Detect unauthorized activity on AMP's network.

AMP's IT Provider recommended to AMP that it purchase a network attached storage device ("**NASD**") to store backup data. On June 21, 2016, AMP's IT Provider installed such a device; however, the IT Provider did not identify during installation that the NASD featured a software protocol (called "remote synchronization") that allowed for permission-less access to the NASD's contents from the Internet. From the date of installation through April 17, 2017, AMP's customers' records and information stored on the NASD were left unprotected because of this software protocol. In April 2017, an unauthorized third party accessed AMP's IT network and copied approximately 97,000 files including customer records and information containing personally identifiable information. The order noted that AMP's IT Provider's risk assessments of access routes to AMP's network and quarterly risk assessments to identify vulnerabilities did not identify the NASD's vulnerability. The IT Provider failed to note the NASD's vulnerability despite media reports on three other incidents of unauthorized access of NASDs used by other organizations, including some from the same manufacturer of AMP's NASD. The CFTC ultimately faulted AMP for its IT Provider's failures and the resulting breach.

The Takeaways. This action highlights that regulators plan to hold the companies they supervise responsible for poor cybersecurity practices. Like AMP, companies cannot escape their obligation to develop a robust cybersecurity program by delegating to an unregulated third-party service provider. This is true for companies that are subject to a new NYDFS cybersecurity rule, which required a senior officer or board member to certify compliance with the company's cybersecurity obligations earlier this month. And this is increasingly the case for companies that are subject to older rules, like Regulation 166.3, that have been retooled for cybersecurity issues. Companies must keep this in mind as their reliance on third-party service providers for cybersecurity, such as cloud providers, increases.

Of note, the CFTC adopted Regulation 166.3 in 1983 to ensure that FCMs maintained responsibility for their customers' information when partnering with introducing brokers. The CFTC's use of Regulation 166.3 to assert that FCMs must supervise their IT providers serves as yet another example of regulators repurposing long-established rules to establish and enforce cybersecurity obligations, like **states using their consumer protection statutes that prohibit deceptive trade practices in cases brought against Equifax**.

Daniela Dekhtyar-McCarthy contributed to this post.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Gabriel D. Rosenberg
+1 212 450 4537
gabriel.rosenberg@davispolk.com