BARNES & THORNBURG LLP

Cybersecurity: CFTC Brings Enforcement Action For Faulty IT System

February 19, 2018 | Privacy,The GEE Blog

Trace Schmeltz
Partner
Financial and Regulatory Litigation Group
Co-Chair, Fintech Co-Chair

This past week, the Commodity Futures Trading Commission (CFTC) settled an enforcement action in which it had alleged that futures commission merchant AMP Global Clearing LLC violated 17 C.F.R. 166.3 (duty of supervision) by failing to diligently supervise implementation of a critical component of its information systems security program (ISSP). As a result, AMP suffered a cybersecurity breach that led to loss of nearly 100,000 files, including customers' personal identifying information. As a result of the settlement, AMP paid a $100,000 fine and, undoubtedly, faces significant other expenses in dealing with the customers for whom it lost private information. AMP will also have to provide written verification to the CFTC of its efforts to strengthen its network security and ensure compliance with its ISSP.

What Happened? AMP hired a vendor to install a NASD (network attached storage device) that, unbeknownst to AMP, had a backdoor that allowed access to the NASD over the Internet. The "backdoor" could allow intruders to copy information from the NASD. Apparently, neither AMP nor its IT provider found this backdoor in their quarterly risk assessments—which included network penetration tests, vulnerability scans and firewall audits.

RELATED PRACTICE AREAS

Financial and Regulatory Litigation
Government Litigation
Securities and Capital Markets
White Collar and Investigations

POPULAR TAGS

Commodity Futures Trading Commission (CFTC)
Cyber Insurance
information systems security program
network attached storage device

What Should Have Happened? AMP's IT vendor should have uncovered this backdoor in its quarterly risk assessments. It is possible that the vendor's assessments were not sufficiently robust. Or, perhaps the vendor knew the backdoor existed but left it there for maintenance purposes. After all, the feature was intended to allow another NASD to copy information out of the NASD on AMP's system. Such a feature could allow data recovery for a failing NASD.

In addition, AMP's own people should have—at least, the CFTC suggests they should have—figured out that the NASD they installed was prone to these types of security failures. In fact, the CFTC's press release on the matter states that "the media had reported three other incidents of unauthorized access of NASDs used by organizations other than AMP, including some from the same manufacturer of AMP's NASD." In other words, a little bit of research could have prevented this problem.

Either way, what certainly should have happened (and we simply do not know whether or not it did based on publicly available data) is AMP should have negotiated an indemnification provision in the contract with its IT provider, holding AMP harmless from any and all expenses (including the fine from the CFTC) resulting in the IT provider's negligence. And, AMP and the IT provider should have had robust cybersecurity insurance to cover the loss.

What is Next? AMP has to provide two written follow-up reports "verifying AMP's ongoing efforts to maintain and strengthen the security of its network and its compliance with its ISSP's requirements." This action suggests that every CFTC registrant (except associated persons without supervisory duties) review its information systems security program, consider whether its network is vulnerable based on the hardware being used, review its contracts with its IT providers, and double-check the coverage afforded by its cyber-security insurance.