BRACEWELL

INSIGHTS

Who Is Watching The Watchmen?: CFTC Penalizes Registrant For Outsourced IT Security Lapses

March 12, 2018

By: ***Michael W. Brooks***

On February 12, 2018, the Commodity Futures Trading Commission (CFTC) settled charges against AMP Global Clearing LLC (AMP), a futures commission merchant (FCM), for the company's failure to adequately supervise one of its IT providers, which led to the unauthorized access of nearly 100,000 customer records by a third party.[1] In order to settle the enforcement action, AMP agreed to a $100,000 civil penalty and to provide written reports to the CFTC "verifying AMP's ongoing efforts to maintain and strengthen the security of its network and its compliance with its ISSP's requirements." This order is a reminder to all CFTC registrants – including but not limited to FCMs, commodity trading advisors (CTAs), commodity pool operators (CPOs) and swap dealers – that they bear the responsibility for protecting customer information.

Background

AMP hired an unnamed IT provider to implement provisions of AMP's information systems security program ("ISSP"), including the performance of risk assessments, maintenance of the AMP's firewall, and detection of unauthorized activity on AMP's network. In June 2016, during the installation of a new storage device, the IT firm created an open access route from the Internet through the company's firewall to the new storage device. As a result, information regarding AMP's customers, including personally identifiable information, could be openly accessed on the internet. The IT firm did not perform a risk assessment on the new storage system and on a quarterly basis informed AMP's officers that there were no network security concerns based on the firm's periodic network penetration tests, vulnerability scans, and firewall audits. In March 2017, the unprotected information was discovered by a third party and in April 2017, undetected by AMP, the third party copied approximately 97,000 files from the storage system. One week later, the third party contacted AMP and federal authorities to inform them about the breach. AMP immediately removed the storage device and began an internal investigation to determine the scope of the compromise.

The CFTC Order

In its Order, the CFTC concludes that the "IT Provider's failure to implement fully the ISSP left unprotected against cyber-exploitation a significant amount of customer information, over a multiple month period." By failing to diligently supervise the IT firm's implementation of ISSP provisions, AMP violated Regulation 166.3,[2] which requires registrants to diligently supervise the activities of their agents relating to their business as a CFTC registrant. While maintaining the position that "[a] violation of Regulation 166.3 is an independent violation for which no

underlying violation is necessary," the CFTC identified the activities at issue as relating to Regulation 160.30,[3] which requires registrants to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information."

The CFTC's order concludes the evidence of AMP's failure to supervise is simply the fact that a vulnerability and breach went undetected for nearly ten months, explaining, "for nearly ten months, a significant amount of Respondent's customers' records and information were unprotected and vulnerable to cyberexploitation -- a vulnerability, and ultimately a breach, of which Respondent was unaware until being notified by the Third Party." The CFTC Order recognizes AMP's substantial cooperation and remediation during the investigation and states that the civil penalty reflects this cooperation.

Takeaways

Whether accomplished through a third-party vendor or directly, registrants must undertake to comply with both their obligations pursuant to Regulations 166.3 and 160.30 with respect to cybersecurity. This action highlights the risk that registrants that delegate ISSP administration to third party vendors may be held liable in the event the vendor does not perform its contractual obligations by failing to detect a system flaw. The CFTC has set a high bar for registrants in the supervision of their vendors and demonstrates that taking vendors at their word is not sufficient. Registrants should ensure that they maintain robust ISSPs and diligently supervise vendors tasked with their policies' implementation.

---

[1] The CFTC Order settling the charges is available ***here***.

[2] https://www.gpo.gov/fdsys/pkg/CFR-2014-title17-vol2/pdf/CFR-2014-title17-vol2-sec166-3.pdf

[3] ***https://www.gpo.gov/fdsys/pkg/CFR-2004-title17-vol1/pdf/CFR-2004-title17-vol1-sec160-30.pdf***