Akin®

CFTC Settlement Asserts Data Breach Disclosure Requirement for Future Commission Merchants

Oct 11, 2019

Reading Time : **3 min**

By: Jason Daniel

The settlement is the second cybersecurity action settled by the CFTC and is the largest to date. Settling for $100,000, the earlier action involved claims that a FCM's inadequate supervision of an information technology provider caused that entity's computer systems to be compromised by an unauthorized third party.

The settlement offers critical guidance on data security practices and disclosure requirements for FCMs and other CFTC registrants.

I. Supervisory Violations

CFTC Regulation 166.3 imposes a broad duty on all CFTC registrants, including FCMs, to "diligently supervise the handling . . . of all commodity interest accounts carried, operated, advised or introduced [it] by the registrant and all other activities of its partners, officers, employees, and agents . . . ." [1] In the data security context, Regulation 160.30 requires FCMs to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of customer records and information." [2] Applying these two requirements together, the CFTC may hold FCMs accountable for failures to "diligently supervise" how these policies and procedures are implemented and how customer records and information are protected.

The CFTC found that PCI failed to meet this standard with respect to its cybersecurity policies and practices. As an initial matter, PCI failed to tailor its information system security program (ISSP) to the scope and particular risks of its operations. Rather, the Company's ISSP

employed, verbatim, the boilerplate language included in a National Futures Association Interpretive Notice that required the establishment and implementation of ISSPs. Making matters worse, at the time of the phishing attack, the Company had no individual person responsible for administering its ISSP. Instead, PCI had assigned the responsibilities of administering the program amongst a number of employees who were "not adequately qualified to take over cybersecurity responsibilities." In the aftermath of the phishing attack, no Company personnel consulted the ISSP to determine next steps.

The consent order also notes PCI's supervisory failures with respect to its disbursement policies. Again, the Company failed to adequately maintain written policies on the subject; instead, the Company held its disbursement policy within a spreadsheet that it used to track disbursements. According to those procedures, Company staff are to confirm wiring instructions with a confirmatory call to the customer. Still, rather than consulting this policy, the customer service specialist who received the fraudulent email consulted a supervisor and then the Company's Chief Compliance Officer (CCO) as to the propriety of the request. Failing to refer the staffer to the Company's disbursement policy, the CCO approved the transfer on the condition that the customer was requesting the funds to send to one of the customer's own clients. The customer service specialist executed the transfer after confirming the purpose of the distribution with the cyber criminals over email.

II. Disclosure Violations

Regulation 1.55(i) requires FCMs to disclose to current and potential customers "all information about the [FCM], including its business, operations, risk profile, and affiliates, that would be material to the customer's decision to entrust such funds to and otherwise do business with the [FCM]." 17 C.F.R. § 1.55(i) (2018).

The CFTC found that PCI violated this regulation in its attempts to keep news of the breach from customers. Particularly, PCI's leadership "ultimately determined not to inform their customers of the cybersecurity breach or the fraudulent wire transfer, and instead sent a non-specific warning to PCI customers about phishing schemes in general." Only after the CFTC's Division of Swap Dealer and Intermediary Oversight "repeatedly" point out the Company's disclosure obligations under CFTC Advisory 14-21 did the Company endeavored to investigate either the scope of customer information compromised by the phishing attack or the existence of any other fraudulent transfer requests.

The CFTC concluded that the successful phishing scheme, the transfer made on the basis of the fraudulent request, and the Company's failure to identify the scope of affected customer information were, collectively, information that was "material to a customer's decision to entrust its funds and do business with" PCI and therefore should have been disclosed.

CFTC Cybersecurity Enforcement: The Road Ahead

The consent order reached with CPI is the first to find that the fact of a cybersecurity event is "material information" giving rise to a disclosure obligation on part of a FCM. Going forward, FCMs should include disclosure to customers as part of their response to any cyber event.

Prior to any breach, FCMs should maintain a practice of regularly reviewing their ISSP to ensure that the program is tailored to their particular line of business and associated risks. Review of this document and execution of its policies should be the responsibility of an identified staff person at the FCM with sufficient cybersecurity expertise to administer the ISSP.

Finally, FCMs should ensure that firm policies beyond the ISSP are drafted and administered with an eye to cybersecurity threats.

[1] 17 C.F.R. § 166.3 (2018)

[2] 17 C.F.R. § 160.30 (2018)

Categories

Cybersecurity & Information Security | Financial Data Privacy