September 23, 2019

CFTC Fines Phillip Capital for Failure to Prevent a Cyber Attack That Resulted in the Theft of Customer Funds

CFTC Also Finds That Cyber Attack was Material Information That Should Have Been Disclosed to Customers

On September 12, 2019, the Commodity Futures Trading Commission ("CFTC") issued a consent order against Phillip Capital, Inc. ("Phillip"), a Chicago-based Futures Commission Merchant, requiring payment of a $500,000 penalty and $1 million in restitution.[1] In early 2018, cyber criminals gained access to Phillip's email system using a phishing attack, and then used customer information they obtained to convince Phillip personnel to transfer $1 million from a customer account to a bank in Hong Kong. Phillip wired the funds, and did not realize that the wire request was fraudulent until the customer whose funds had been wired alerted Phillip. The CFTC determined that Phillip failed to diligently supervise its employees with respect to their implementation of cybersecurity and funds disbursement procedures. The agency further found that Phillip violated applicable regulations by failing to inform its customers about the cyber attack and the resulting funds transfer, which facts the CFTC believed would have been material to current and prospective customers.

This is the CFTC's second cybersecurity enforcement action[2] and reflects an increasing trend among regulators to hold companies victimized by cyber criminals accountable for failing to prevent the attacks. This enforcement action also has a less common element, where the regulator determined that the cyber attack indicated a material risk that should have been disclosed to customers.

The Cybersecurity Breach and the $1 Million Wire Transfer

On February 28, 2018, Phillip's IT Engineer received a phishing email, clicked on the attachment, and entered login information for a Phillip administrator's email account in order to access the document. The cyber criminals were able to use these credentials to access email accounts for Phillip's co-CEO and various Phillip finance employees, which contained detailed customer information. Although the IT Engineer noticed that the compromised email accounts had been added as a delegate to his email account the next day, and removed that delegation, he did not realize that his email account had been compromised until March 2, 2018, when the delegation was restored. At that point, he reset the password to his email account, informed management of the breach, and advised other Phillip employees to change their email passwords. However, although Phillip had adopted a written Information System Security Program ("ISSP"), neither he nor anyone else at Phillip consulted the ISSP at the time of these events.

On March 2, the same day that the IT Engineer realized that his email account had been compromised, the cyber criminals emailed Phillip posing as a Phillip customer and requested that $1 million be wired from the customer's account to a bank in Hong Kong. According to the CFTC's order, Phillip personnel failed to follow procedures that would have required a phone call to the customer to confirm the transfer. Instead, Phillip personnel asked for confirmation that the recipient of the wire was one of the customer's clients. The criminals so confirmed and Phillip sent the funds.

On March 5, the customer called to ask why $1 million had been wired from its account, thereby alerting Phillip that the wire request was fraudulent. Phillip then took steps to preclude additional transfers, notified the CFTC, and reimbursed the customer for the $1 million that had been improperly disbursed.

The CFTC found that Phillip had violated CFTC Regulations 166.3 and 160.30.[3] According to the CFTC, the ISSP adopted by Phillip was not reasonably tailored to its operations, and Phillip's supervisors failed to assign an adequately qualified employee to oversee the ISSP and to oversee the actions of its employees in implementing and following cybersecurity policies. In addition, Phillip did not have compliance personnel who could knowledgeably assess its cybersecurity policies and procedures. These shortcomings were highlighted by Phillip's failure to consult its ISSP following the security breach, and by its failure to grasp the importance of assessing the scope of the breach and its effects on customer data.

The Failure to Notify Customers

Following the cybersecurity breach and fraudulent transfer, Phillip management considered what, if anything, it should disclose to its customers regarding these events. The company decided not to inform its customers, but instead sent a non-specific warning to its customers about phishing schemes in general. Indeed, the company took efforts to keep the fact of the breach from its customers and the public, with the company's co-CEO noting in a company-wide email that "this is all confidential and no mention should be made outside the company – this is very important and could affect the company."

Following an investigation, Phillip determined that the cyber criminals had obtained the information of a second customer, and Phillip alerted that customer. Phillip could not, however, determine whether the criminals had viewed other customers' information, and it decided not to inform other customers on that basis.

The CFTC found that Phillip's failure to disclose the facts of the breach and the fraudulent wire transfer in a timely manner to all of its customers was a violation of CFTC Regulation 1.55(i).[4] That information, the CFTC reasoned, would have been material to customers' decision-making. As the CFTC explained:

- The facts that [Phillip] was subject to a cybersecurity attack that compromised customer information, and then, following that attack, honored a fraudulent request to wire $1 million in customer funds, and could not determine the scope of compromised customer information, is information that would be

> material to a customer's decision to entrust its funds and do business with [Phillip]. Indeed, the fact that [Phillip] took steps to safeguard these facts in order to protect its reputation demonstrates the materiality of this information.

Implications

This is the second enforcement action in which the CFTC has held a regulated entity accountable for failing to implement or follow appropriate cybersecurity procedures, thereby allowing outsiders to obtain access to client funds or information. The Securities and Exchange Commission has taken several enforcement actions in this vein, which have held broker-dealers or investment advisors liable for failing to interdict external or internal cyber threats.[5] Although we have not yet seen a significant enforcement action by banking regulators to similar effect, financial institutions of all kinds should be increasingly prepared to face enforcement when they are victimized by cyber criminals.

Further, this enforcement action puts FCMs on notice that, depending on the facts and circumstances, a cyber attack may rise to the level of material information that needs to be disclosed to existing and prospective customers. FCMs should consider incorporating this issue in their incident-response procedures.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Roberto J. Gonzalez
+1-202-223-7316
rgonzalez@paulweiss.com

Udi Grofman
+1-212-373-3918
ugrofman@paulweiss.com

Jeh Charles Johnson
+1-212-373-3093
jjohnson@paulweiss.com

Jonathan S. Kanter
+1-202-223-7317
jkanter@paulweiss.com

Brad S. Karp
+1-212-373-3316
bkarp@paulweiss.com

Marco V. Masotti
+1-212-373-3034
mmasotti@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Richard C. Tarlowe
+1-212-373-3035
rtarlowe@paulweiss.com

Lindsey L. Wiersma
+1-212-373-3777
lwiersma@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

---

1 This client alert describes the allegations contained in the order, which Phillip did not admit or deny. *See* Phillip Capital, Inc., CFTC No. 19-22 (Sept. 12, 2019), available at https://www.cftc.gov/media/2476/enfphillipcapitalincorder091219/download.

2 *See* AMP Global Clearing LLP, CFTC No. 18-10 (Feb. 12, 2018), available at https://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfampglobalorder021218.pdf.

3 Regulation 166.3 requires Commission registrants to "diligently supervise the handling . . . of all commodity interest accounts carried, operated, advised or introduced by the registrant . . . relating to its business as a registrant." 17 C.F.R. § 166.3 (2018). Regulation 160.30 requires Futures Commodity Merchants ("FCMs") like Phillip to "adopt policies and procedures that address administrative, technical and physical safeguards for the protection of consumer records and information." 17 C.F.R. § 160.3 (2018); *see also* Commission Staff Advisory No. 14-21, February 26. 2014 (enumerating "best practices" for safeguarding customers' records in according with Regulation 160.30; and National Futures Association Interpretive Notice 9070 (effective March 1, 2016 and updated April 1, 2019) (establishing general requirements relating to registrants' Information System Security Programs). The National Futures Association is the industry-wide self-regulatory organization designated by the CFTC to regulate derivatives markets. *See* https://www.nfa.futures.org/about/index.html.

4 CFTC Regulation 1.55(i) requires FCMs to disclose to their 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 and otherwise do business with the FCM." 17 C.F.R. § 1.55(i) (2018).

5 *See, e.g.*, Voya Financial Advisors, Inc., No. 3-18840 (Sept. 26, 2018), available at https://www.sec.gov/litigation/admin/2018/34-84288.pdf; Morgan Stanley Smith Barney LLC, No. 3-17280 (June 8, 2016), available at https://www.sec.gov/litigation/admin/2016/34-78021.pdf; U.S. Sec. & Exch. Comm'n, Press Release, SEC Charges

Investment Adviser with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach (Sept. 22, 2015), available at https://www.sec.gov/news/pressrelease/2015-202.html.