Failure to Prevent a Business Email Compromise, and to Notify Customers of It, Gives Rise to Sanctions Against Victim Company

September 18, 2019

The Commodity Futures Trading Commission ("CFTC") brought and settled a $1.5 million enforcement action against Phillip Capital Inc. ("Phillip"), a registered futures commission merchant, after an IT employee gave up login credentials in response to a phishing email. After gaining access to the IT employee's email account, the hackers leveraged that access to view other employees' emails.

Using information gleaned from the emails, the cyber criminals posed as a Phillip customer and crafted a bogus wire request for $1 million. Upon receipt of the wire request, a Phillip employee consulted supervisors to determine the appropriate procedure for verifying the request. Though Phillip's procedures required a confirmatory phone call, the employee instead sought confirmation by email—thereby unwittingly responding to the hackers, who confirmed the validity of the request. This resulted in $1 million of the customer's money being sent to a Hong Kong bank account controlled by the hackers.

The CFTC found Phillip violated Commission Regulations 160.30 and 166.3, which required Phillip to adopt policies to protect customer information; to diligently supervise the implementation of those policies and safeguards; and to diligently supervise all customer accounts and ensure the detection of wrongdoing. The CFTC asserted:

- Phillip adopted a written information systems security program that was not reasonably tailored to its operations and even copied generic language from a model template published by the National Futures Association.

- When the IT employee tasked with overseeing the security program departed the firm, Phillip did not hire a replacement or assign an adequately qualified new employee to take over cybersecurity responsibilities.

- Employees were not adequately trained regarding Phillip's own disbursement policies, as evidenced by the employee's use of email—rather than a phone call—to confirm wiring instructions.

- Phillip did not have compliance personnel who could knowledgably assess the adequacy of its policies and procedures relating to cybersecurity, as evidenced by Phillip's failure to consult its own security program following the breach or to fully investigate the breach in a timely manner.

The CFTC also found Phillip violated Commission Regulation 1.55(i), which requires firms to disclose information "that would be material to the customer's decision to entrust [its] funds to and otherwise do business with the [firm]." The CFTC found "management made concerted efforts to keep the fact of the breach from its customers and the public," citing internal documents in which an executive cautioned employees that "this is all confidential and no mention should be made outside the company—this is very important and could affect the company" and separately directed another executive to ask any customers who may have learned of the breach not to discuss it with others, as "it will only hurt our company for others to know and it to be talked about."

These findings may have been prompted, in part, by the CFTC's view that the firm "did not prioritize determining the impacts of the breach on customer information." According to the CFTC, "[i]n discussions with the Commission in the days and weeks following the breach . . . [CFTC] repeatedly highlighted customer disclosure obligations." The CFTC stated that "[o]nly then did Phillip investigate what customer information may have been compromised," assigning the investigation to the same IT employee who had initially fallen for the phishing attempt without seeking the assistance of outside experts.

The subsequent investigation identified that the hackers searched for two customers' names in the email accounts. The CFTC criticized Phillip's decision to notify just those two customers, noting that Phillip "could not know the extent of compromised customer information" and rejecting Phillip's "rationale that it had no affirmative evidence" that other customers' accounts were viewed. The CFTC concluded that Phillip had an obligation to notify all of its current and prospective customers of the incident (which Phillip ultimately did).

This finding is particularly noteworthy for those who experience compromises of email accounts where it may be difficult or impossible to determine which particular emails a hacker may have viewed. The CFTC's position evidences regulatory skepticism that notification obligations can be limited on the basis that a company lacks affirmative evidence that hackers accessed particular emails. Rather, depending on the circumstances, a more robust investigation may be needed before reaching the conclusion that limited notifications are appropriate.

CLOSING THOUGHTS

- It has been a familiar feature of cybersecurity law that civil regulators do not hesitate to penalize hacking victims where the victims' pre-breach security posture or post-breach response is seen as inadequate. This case extends that principle to business email compromise—one of the most widespread forms of cyberattack affecting companies across all economic sectors.

- This action is yet another reminder that regulators expect cybersecurity policies and procedures to be detailed, specific, tailored to the enterprise and adhered to during an actual incident. Off-the-shelf, generic policies are not enough, and training is necessary to ensure policies are actually followed.

- Companies also need to make sure that individuals filling key roles, including information security roles, have the necessary skills and training for the job—even if they are only filling the role on an interim basis.

- In the absence of a robust investigation, regulators may be skeptical of a company's decision to narrowly circumscribe breach notifications. Careful consideration will need to be given to the full state of the forensic evidence before deciding that the absence of evidence can justify narrowing the customers to whom breach notifications are provided.

* * *

Our Cybersecurity and Data Privacy team would be pleased to discuss these issues further with our clients and friends.

Please do not hesitate to contact us with any questions.

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

Christopher S. Ford
csford@debevoise.com

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Jaime Freilich
jmfreilich@debevoise.com

Jim Pastore
jjpastore@debevoise.com