Client Update
A Cybersecurity Fine From FINRA

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Jim Pastore
jjpastore@debevoise.com

Lee Schneider
lschneider@debevoise.com

Gabriel W. Lezra
gwlezra@debevoise.com

WASHINGTON, D.C.
Luke Dembosky
ldembosky@debevoise.com

What was broker-dealer Lincoln Financial Securities Corporation expecting when it decided, as so many businesses reasonably do, to turn customer data over to a third-party vendor for hosting in the cloud? Probably not that if the *vendor* got hacked, the Financial Industry Regulatory Authority would bring the hammer down on *Lincoln*. But that is just what FINRA recently did, fining Lincoln $650,000. The case vividly shows how cybersecurity enforcement authorities may seek to hold a firm liable after the fact, even when the firm itself is the victim of a criminal hack.

Back in 2011, a Lincoln supervisory office began to store client records with a cloud vendor. The stored documents included customers' Social Security numbers and other nonpublic personal information. In 2012, a hacker broke into the cloud vendor's systems. FINRA's summary of the case states that the hacker exposed the information of over 5,400 Lincoln customers.

What supported the fine of Lincoln in FINRA's view, and what can the case teach companies in and out of the securities industry?

FINRA's findings:	**Potential lessons:**:
In 2011, FINRA fined two Lincoln entities a total of $600,000 for allegedly failing to secure their web-based electronic portfolio management systems. In connection with the 2016 fine, FINRA concluded that Lincoln—following the 2011 fine—did not adopt "written supervisory procedures," or WSPs, that were "reasonably designed" to ensure the security of customers' confidential	Enforcement authorities can be particularly tough the second time around. The Federal Trade Commission did not go easy on Wyndham Hotels when it experienced multiple data breaches. Fairly or not, FINRA seems to have taken a tough approach when investigating Lincoln a second time. It bears mention that the Cybersecurity Framework promulgated by the National Institute

information. Such WSPs are required under FINRA rules and were required at the time under the then-relevant rules of the National Association of Securities Dealers.	of Standards and Technology (NIST), a leading set of cybersecurity standards, suggests that "[r]ecovery planning and processes [be] improved by incorporating lessons learned [from a breach] into future activities."
FINRA concluded that Lincoln's cloud vendor did not use certain cybersecurity measures—specifically, the vendor did not use properly installed antivirus software, nor did the vendor encrypt the stored personal information—and that Lincoln had not ensured the vendor would use these measures.	Enforcement authorities increasingly believe that certain cybersecurity measures are sufficiently well-recognized that *not* to use them can be deemed unreasonable—*i.e.*, contrary to legal standards. Here, FINRA cited the alleged absence of appropriate antivirus and encryption measures at the cloud vendor. In other cases from the FTC, enforcement agencies and courts, various other shortfalls in cybersecurity have been alleged—such as the lack of multifactor authentication.
FINRA concluded that Lincoln had not sufficiently supported the cybersecurity of its registered representatives. For example, according to FINRA, a Lincoln data security policy required that representatives install firewalls. But, FINRA said, the policy did not describe what type of firewall should be used or how to install it. FINRA thus regarded the policy as not meeting the standards for a WSP.	FINRA apparently sees the brand-name, "mother ship" company as having highly specific obligations that extend throughout the network. One might think that a company atop a decentralized network should not be legally obligated to give paint-by-numbers instructions for functions like firewall selection and installation. At least in this case, however, FINRA concluded that Lincoln had a duty to be more prescriptive.

FINRA determined that some of Lincoln's registered representatives also engaged vendors to host customer data. But according to FINRA, Lincoln did not monitor or audit the cybersecurity practices of these vendors. FINRA deemed such oversight to be required as part of a FINRA member's "continuing responsibility" under Notice to Members 05-48 to engage in vendor oversight.	At least in FINRA's view, policing the cybersecurity of vendors has gone from best practice to legal obligation. While FINRA was tough on Lincoln here, the issue is not limited to the securities industry. The breaches at Target, Ashley Madison, and the Office of Personnel Management, to name just a few, happened after vendors' credentials were compromised. Options for companies looking to upgrade their vendor oversight might include pre-engagement due diligence, enforcing a rigorous program of access controls, and ongoing testing and verification of vendors' security.
Importantly for Lincoln and its customers, FINRA acknowledged that Lincoln was unaware of any actual misuse of the customer data from the breach in 2012 of the cloud vendor engaged by Lincoln's supervisory office. The additional cloud vendors engaged by registered representatives of Lincoln were not even breached.	At least in FINRA's eyes, neither customer harm nor a breach is necessary to impose cybersecurity sanctions. FINRA cited the purported lack of "reasonable" WSPs, and the purported failure to supervise, as enough in this case to support liability. It is worth noting that FINRA's aggressive posture may not hold in the law generally. For example, a recent federal appeals court decision suggests that more rigorous proof of harm may be required before the FTC can deem a hacked company's cybersecurity to be an unfair business practice under Section 5 of the FTC Act.

FINRA noted that Lincoln operated through a network of over 500 branches and over 1,100 registered representatives.	Companies operating in a highly decentralized manner are not immune from cyber risk at the far reaches of their business. Many financial services firms use a decentralized model similar to Lincoln's. One can reasonably ask: How fair or practical is it to expect such a company to promote and enforce cybersecurity standards throughout its decentralized network—even to vendors engaged by representatives in distant branch offices? Yet this case indicates that FINRA, at least, seemingly stands ready to impose liability on that basis.

* * *

Please do not hesitate to contact us with any questions.