LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

SEC Cyber Actions A 'Wake-Up Call' For Brokers, Advisers

By **Al Barbarino**

Law360 (August 31, 2021, 7:57 PM EDT) -- The U.S. Securities and Exchange Commission's latest cybersecurity-related enforcement actions are being seen as a "wake-up call" for broker-dealers and investment advisers who may be cutting corners, showing the agency's exam and enforcement units are now working in full lockstep to protect customers and their data.

The agency on Monday announced it had hit a group of brokers and advisers with hundreds of thousands of dollars in fines, alleging in three separate orders that the firms had taken inadequate steps to protect customer data.

In the announcement, the chief of the SEC's cyber unit, Kristina Littman, warned brokers and advisers about taking shortcuts when it comes to cybersecurity.

"It is not enough to write a policy requiring enhanced security measures if those requirements are not implemented or are only partially implemented, especially in the face of known attacks," Littman said.

The agency hit Cetera Financial Group and associated entities with a $300,000 fine, Cambridge Investment Research Inc. and a related entity with a $250,000 fine, and KMS Financial Services Inc. with a $200,000 penalty.

Vivek Mohan, a partner in Mayer Brown's cybersecurity and data privacy practice, noted the latest actions are "the product of several years of maturing thought on how the SEC can play a role when evaluating the adequacy of cyber controls."

The agency has been focused on cybersecurity issues for many years. Former Chairman Jay Clayton created the dedicated cyber unit within the Enforcement Division, which ultimately helped bring charges in 2018 against Yahoo for allegedly failing to disclose a large data breach.

The actions also come amid broader elevated sensitivity surrounding cybersecurity issues following a pandemic that exposed deep vulnerabilities, a number of high-profile hacks of both government agencies and private companies, and executive orders by President Joe Biden seeking to step up the U.S.' response to those hacks.

In June, the SEC requested information from what was likely hundreds of public companies regarding their potential exposure to the SolarWinds cyberattack, a move that sent firms scrambling to gather the relevant information on a short deadline.

But while public companies often grab headlines, the agency has been issuing risk alerts and other communications to broker-dealers and advisers about cybersecurity as far back as September 2015, when its then-Office of Compliance Inspections and Examinations announced a so-called cybersecurity exam initiative.

"They've given these entities reasonable notice, and we're now seeing the results borne out," Mohan said. "This is a good wake-up call for those who haven't spent enough time on this."

Monday's announcement featured a long list of SEC examinations staff who helped uncover the alleged violations, demonstrating that the agency's exam and enforcement units are working in full lockstep to uncover potential breaches.

"The exam unit's staff has improved its understanding of cyber risks and is applying that in examinations," said James Lundy, a partner with Faegre Drinker Biddle & Reath LLP and former senior regulatory counsel with the SEC.

The SEC cited violations of the so-called safeguards rule against all three firms and, in the case of Cetera, breaches of the Advisers Act.

The former rule requires registrants to have written policies and procedures that protect customer records and information, while the element of the Advisers Act cited requires policies and procedures dictating the "review of communications to advisory clients."

"This failure resulted in sending breach notifications to the firms' clients that included misleading template language suggesting that the notifications were issued much sooner than they actually were after the discovery of the incidents," according to the Cetera order.

According to the orders, the Cetera entities' cloud-based email accounts of over 60 personnel were taken over by unauthorized third parties, resulting in the exposure of personal information of at least 4,388 customers and clients.

"None of the taken-over accounts were protected in a manner consistent with the Cetera entities' policies," the SEC said, adding that the firms sent breach notifications to clients that included "misleading language."

The agency, meanwhile, said the cloud-based email accounts of over 121 Cambridge representatives were taken over by unauthorized third parties, exposing the information of well over 2,000 customers and clients.

The firm had "failed to adopt and implement firm-wide enhanced security measures for cloud-based email accounts," the SEC said.

Lastly, in the case of KMS, the firm's cloud-based email accounts resulted in exposure of the information of 4,900 KMS customers and clients, and the firm "failed to adopt written policies and procedures requiring additional firm-wide security measures."

None of the firms admitted or denied the findings as part of the settlement.

Lundy said the SEC is making clear that firms must do everything possible to protect customer information, while also working closely with chief information officers and others in communications roles to disclose potential breaches accurately and timely.

The agency is now "using the whole toolbox of regulatory tools" it has to clamp down on firms that may be cutting corners, including other recent actions against financial firms, Mohan added.

In June, the SEC announced settled charges against title insurer First American Financial Corporation in one of the first instances in which the agency brought charges in the absence of an actual data breach, instead focusing solely on whether the issuer's policies and procedures were adequate.

And in May, the agency announced that a broker-dealer arm of Empower Retirement would pay a $1.5 million fine for allegedly failing to file hundreds of suspicious-activity reports despite knowing that its customer accounts were the subject of a potential hack.

While the agency is targeting this coming October for a rule proposal addressing cybersecurity risks among public companies, which was mentioned in a regulatory agenda earlier this year, there is no proposed rulemaking related to broker or advisers imminent.

But a new rule might not be needed, experts said. In fact, the agency "is only scratching the surface" with regard to its ability to enforce cybersecurity based on existing rules and regulations, Mohan said.

Lundy called SEC Chairman Gary Gensler "one of the more sophisticated chairs … in terms of the intersection of technology and securities laws," making him the appropriate figurehead to oversee the potential rulemaking both on the public company and investment advisory side.

But Lundy agreed that Monday's actions, particularly the intertwining of cybersecurity issues with regulatory staples like the Advisers Act, show the SEC doesn't necessarily need any new rulemaking to step up enforcement.

"They've made it pretty clear that they can enforce cybersecurity based on the laws that are already on the books," Lundy said.

--Editing by Philip Shea.
