CARLTON FIELDS

Making Good on Its Promise: SEC Pursues Cyber Enforcement Actions Against Financial Services Companies

CYBERSECURITY AND PRIVACY | INSTITUTIONAL INVESTMENT AND FINANCE | SECURITIES & INVESTMENT COMPANIES | SECURITIES INQUIRIES, EXAMINATIONS & ENFORCEMENT | SECURITIES AND DERIVATIVE LITIGATION | OCTOBER 4, 2021


Joseph W. Swanson


Michael L. Yaeger


Eden Marcu

On August 30, the Securities and Exchange Commission (SEC) announced settled charges with several investment advisory firms and broker-dealers following email account takeovers. These settlements are the latest in a string of enforcement actions relating to what the SEC considers as cybersecurity failures at registered financial firms. The settlements are notable not only for the alleged deficiencies at issue in each matter but also because they herald a robust approach to cyber enforcement by the agency. Representations about cybersecurity are increasingly likely to be considered material by the SEC.

In all three settlements, the SEC found violations of the Safeguards Rule, which requires financial institutions to have measures in place to secure customer information. The penalties in the three settled proceedings ranged from $200,000 to $300,000.

In the action against Cetera Advisor Networks and other Cetera entities, the SEC alleged that those entities did not enforce cybersecurity policies and procedures with their affiliates. The SEC alleged that, as a result, unauthorized third parties accessed cloud-based email accounts of independent contractors at Cetera. The breach was undetected for three years, exposing personally identifying information of more than 4,000 customers. Moreover, despite its disclosure efforts, the Cetera entities issued breach notifications that included what the SEC viewed as misleading language. Without admitting or denying the SEC's findings, the Cetera entities agreed to a penalty of $300,000.

In the action against Cambridge Investment Research Inc. and another Cambridge entity, the SEC alleged that the firms failed to revise their policies and procedures promptly in response to an email account takeover by unauthorized third parties. After the incident, the Cambridge entities suspended the affected accounts and reset passwords, among other things. Although the Cambridge entities first learned of the email account takeover in January 2018, they did not require enhanced security measures until 2021. Given the initiation of the enforcement action despite such remedial measures, the SEC was clearly signaling the importance of enforcing, rather than just implementing, additional security measures in the wake of a breach.

The final action involved KMS Financial Services Inc., and in that action, the SEC pursued an enforcement proceeding in the wake of an email account takeover. Between September 2018 and December 2019, unauthorized third parties allegedly took control of cloud-based email accounts belonging to one of KMS' subsidiary companies, exposing sensitive information of about 5,000 people. The SEC alleged that by failing to adopt and implement written policies and procedures requiring additional firmwide security measures until two years after the incident, KMS did not protect its customer data from being compromised further.

Notably, none of the three actions was alleged to involve unauthorized trades or transfers stemming from the compromises. The SEC's focus on allegedly insufficient policies and procedures and/or the failure to enforce those policies and procedures puts heft behind the agency's many cybersecurity pronouncements and guidance.

As cybersecurity continues to become more important to the financial services industry and its customers, representations about cybersecurity will continue to become more important to industry regulators.

Takeaways

In light of the SEC's actions, registered entities should take the following actions:

- Scrutinize your policies, procedures, and controls with respect to cyber incidents, their remediation, and their disclosure. Are those policies, procedures, and controls not only in place and updated, but enforced?

- Evaluate the status of your “cyber hygiene” and remediate any gaps relative to SEC guidance and enforcement proceedings.
- Where an entity experiences a data breach or similar incident, that entity should carefully consider the accuracy and sufficiency of any disclosures related to that incident. These recent actions show the SEC taking action where it perceives a disclosure was inadequate or misleading.