WINSTON & STRAWN LLP

BLOG

Broker-Dealer/Investment Adviser Charged with Deficient Cybersecurity Practices by the SEC

OCTOBER 4, 2018

The SEC recently charged a registered broker-dealer/investment adviser in connection with a cyber-intrusion that compromised the personal information of thousands of customers. This case is significant because cybersecurity is an area of heightened concern for the SEC and because this is one of the first cases to bring charges against a registered broker-dealer or investment adviser in connection with a cyber-intrusion. *See* Statement on Cybersecurity, Chairman Jay Clayton (September 20, 2017); *see also* SEC Office of Compliance Inspections and Examinations announces 2018 Examination Priorities (February 7, 2018).

The SEC charged the firm with violating Rule 30(a) of Regulation S-P (17 C.F.R. §248.30(a); the "Safeguards Rule") and Rule 201 of Regulation S-ID (17 C.F.R. §248.201; the "Identity Theft Red Flags Rule"). These rules, respectively, require broker-dealers and investment advisers registered with the SEC to adopt written policies and procedures that are reasonably designed to safeguard customer records and information, and require broker-dealers and investment advisers that offer or maintain covered accounts to develop and implement a written Identify Theft Prevention Program. This program is designed to detect, prevent, and mitigate identify theft in connection with the opening of a covered account or any existing covered account.

In its press release announcing this action, the SEC referenced both weaknesses in the firm's cybersecurity procedures and the firm's failure to apply its procedures to systems used by the greater part of its workforce. The firm agreed to pay a $1 million fine. The firm also agreed to retain a compliance consultant to conduct a comprehensive review of the firm's policies and procedures and to implement the recommendations resulting from such review. A copy of the underlying order is available here.

Read our Financial Services & Banking Practice briefing for more on this matter.

TIP: Financial service firms should protect themselves from possible enforcement actions by confirming that their cybersecurity policies and procedures are reasonable and comprehensive and ensure that documented cybersecurity-related red flags receive prompt attention.

2 Min Read

Related Locations

Chicago

New York

Related Topics

Data Breach

Related Capabilities

Tax

Financial Innovation & Regulation

Privacy & Data Security

Related Regions

North America

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.