WILMERHALE

FINRA to Intensify Scrutiny of Cybersecurity Practices at Brokerage Firms

TUESDAY, NOVEMBER 04, 2014

Reuters recently reported that the Financial Industry Regulatory Authority (FINRA) "plans to intensify its scrutiny of cybersecurity practices at brokerage firms in 2015 and is hiring technology savvy examiners to help boost its efforts." FINRA's addition of examiners focused on cybersecurity is one of the most recent in a series of steps taken by regulators and trade groups to evaluate and harden defenses against cyber-attacks.

- In January, FINRA issued Targeted Examination Letters to assess firms' management of cybersecurity threats. The letters addressed:
- - approaches to information technology risk assessment;
  - business continuity plans in case of a cyber-attack;
  - organizational structures and reporting lines;
  - processes for sharing and obtaining information about cybersecurity threats;
  - understanding of concerns and threats faced by the industry;
  - assessment of the impact of cyber-attacks on the firm over the past twelve months;
  - approaches to handling distributed denial of service attacks;
  - training programs;
  - insurance coverage for cybersecurity-related events; and
  - contractual arrangements with third-party service providers.
- In April, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) issued a "Risk Alert" announcing steps being taken by OCIE to assess cybersecurity preparedness in the securities sector. The Risk Alert included a list of sample questions seeking information related to a wide range of cybersecurity issues, including:
- - identification of risks/cybersecurity governance;
  - protection of firm networks;
  - risks associated with remote customer access and funds transfer requests; and
  - detection of unauthorized activity.
- In October, the Securities Industry and Financial Markets Association (SIFMA) published "Principles for Effective Cybersecurity Regulatory Guidance," providing regulators with the

industry's perspective of how to best protect financial industry operations and clients from cyber-attacks. SIFMA's principles include:

- financial services cybersecurity guidance should be harmonized across agencies;
- agency guidance must consider the resources of the firm;
- effective cybersecurity guidance is risk-based and threat-informed; and
- financial regulators should engage in risk-based, value-added audits instead of checklist review.

- Yesterday, the Federal Financial Institutions Examination Council issued a summary of the results of its cybersecurity assessment of over 500 community banks and a recommendation that all regulated financial institutions join the Financial Services Information Sharing and Analysis Center.

FINRA's effort to bolster its cybersecurity examination capability is further evidence of intense and growing concern—in Congress, and among regulators, trade groups and customers—about industry-wide vulnerabilities. In this environment, it is essential that brokerage firms be prepared for both increasingly sophisticated cyber-threats and heightened regulatory scrutiny.

For more information about likely FINRA focus areas or for help designing a self-audit or checklist, please contact Benjamin Powell or one of the following members of our Financial Institutions Cybersecurity Task Force: Reginald Brown and Franca Harris Gutierrez from the Financial Institutions Group; Meredith Cross, Paul Eckert, Bill McLucas, Yoon-Young Lee, Nicole Rabner, and Daniel Schubert from the Securities Department; and Jonathan Cedarbaum, Robert Mueller, Heather Zachary and Aaron Zebley from the Cybersecurity, Privacy and Communications Group.