# SEC and FINRA Release Findings from Cybersecurity Examinations at Brokerage and Advisory Firms

February 4, 2015 Ronald Breaux

PRACTICES Healthcare Transactions and Regulatory, Privacy and Cybersecurity, Energy, Power and Natural Resources, Social Media, Finance, Government and Public Policy, Government Contracts, Healthcare and Life Sciences, Insurance Recovery, Intellectual Property, Investment Management

The SEC's Office of Compliance Inspections and Examinations (OCIE) yesterday issued a Risk Alert reporting its findings from cybersecurity examinations of registered broker-dealers and investment advisers and stated that it will continue its focus on cybersecurity in 2015 through risk-based examinations. OCIE revealed that most of the examined firms had experienced some type of cyber-attack, primarily through malware and fraudulent emails. Given the findings outlined in the Risk Alert, the cybersecurity guidance issued by FINRA and the investor protection tips issued by the SEC's Office of Investor Education and Advocacy yesterday are particularly timely.

In reviewing cybersecurity policies at these firms, OCIE made the following findings:

- The majority of firms maintained written information security policies; conducted periodic, firm-wide cybersecurity risk assessments; conducted firm-wide inventories of technology resources; made use of encryption of some type; and provided their clients with suggestions for protecting sensitive information.
- Many examined firms reported membership in an industry group or organization that existed for the purpose of sharing information related to cybersecurity (for example, the Financial Services Information Sharing and Analysis Center, or "FS-ISAC").
- While many broker-dealers had created a dedicated Chief Information Security Officer position, less than a third of the advisers had done so; instead, advisers would usually assign information security responsibilities to the Chief Technology Officer.
- Most broker-dealers would incorporate cybersecurity requirements into contracts with vendors and business partners, while few advisers did the same.
- Over half of the examined broker-dealers maintained insurance for cybersecurity incidents, while only a small number of advisers maintained insurance that covered cybersecurity incidents.

Similarly, FINRA released a report yesterday identifying effective practices for dealing with cybersecurity threats, based on its 2014 targeted examinations of broker-dealer firms. FINRA "expects firms to consider the principles and the effective practices presented in this report as they develop or enhance their cybersecurity programs." The practices identified by FINRA include:

- Establishing a sound governance framework;
- Utilizing risk assessments and technical controls;
- Developing cyber-incident response plans;
- Managing cybersecurity threats related to vendors and partners;
- Training staff on cybersecurity issues; and
- Participating in intelligence-sharing opportunities.

The SEC's Office of Investor Education and Advocacy also released an Investor Bulletin yesterday providing tips to investors on how to better protect their online investment accounts. These tips include:

- Picking a strong password;
- Using two-step verification for account access; and
- Exercising caution on public networks.

These publications reflect regulators' increased focus on cybersecurity issues. Registered broker-dealers and advisers should take note of these reports and implement appropriate policies to address the identified issues.

For additional information, please contact one of the attorneys listed below.