



Client Memo

Cyber Security Scrutiny Ramps Up: Broker-Dealers and Investment Advisors Subject to SEC Spot Cyber Security Audits; Listed Companies May Face Derivative Actions Following Breaches

It is not without significance that the Securities and Exchange Commission (“SEC”) chose April 15 to issue a Cyber-Security Alert (“Alert”) to broker-dealers and registered investment advisors that indicated it would begin audits of randomly selected firms with regard to information security safeguards. Now that it had the attention of the financial services community, the SEC served notice that it would enforce rules concerning information security by spot audits of broker-dealers and investment advisors as to electronic information safeguards. Notice having been given, with emphasis, these organizations should take the opportunity to shore up their technical and administrative safeguards before the SEC examines them.

Highly publicized breaches of financial information at Target, Michael’s and Neiman Marcus, and losses of personal and financial information by Wyndham Worldwide Corporation, which led to an enforcement action by the Federal Trade Commission, have garnered the attention of the SEC. The SEC sponsored a Cyber Security Roundtable on March 26, and the Alert followed shortly thereafter. The Alert provides a roadmap of areas of concern, and also a template for affected organizations to shore up their cyber security safeguards.

Appended to the Alert is a sample list of requests that the SEC’s Office of Compliance Inspections and Examinations “may” use in audits. Areas of inquiry in the forthcoming audits will include cyber security governance documents and written policies and procedures for information security, including protocols for vendors and other third parties; a document that maps “all network resources, connections and data flows (including locations where customer data is housed);” workforce training on cyber security safeguards; documentation of periodic risk assessments; proof of a data destruction policy; and cyber-risk insurance sufficient to cover potential losses associated with information security risks. The Alert, in this way, posits a blueprint for information safeguards, and broker-dealers and investment advisors should heed the advice and follow the plan set out by the SEC.

Barton LLP | Graybar Building, 18th Floor, 420 Lexington Avenue, New York, NY 10170 | (212) 687.6262 | www.bartonesq.com

Barton LLP prepared this publication to provide information on recent legal developments of interest to our readers. This publication is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. We would be pleased to provide such legal assistance as you require on these and other subjects, please contact the named attorney at the end of the publication or your regular firm contact.

Copyright © 2014 Barton LLP. All Rights Reserved. This publication may not be reprinted or retransmitted, in whole or in part, without the prior written approval of Barton LLP, except that permission is hereby granted to subscribers to photocopy or forward solely for internal use by their attorneys and staff.

ATTORNEY ADVERTISING pursuant to New York RPC 7.1. The choice of a lawyer is an important decision and should not be based solely upon advertisements.

Regulatory scrutiny is not the least of the financial industry's concerns in cyber security. On May 2, a redacted complaint filed in the U.S. District Court of New Jersey stemming from breaches at Wyndham Worldwide Corporation was made public. The complaint alleges the individual defendant directors and officers, "in violations of express promises to the contrary and reasonable expectations failed to take reasonable steps to maintain customers' personal and financial information." Damages to shareholders, the complaint alleges, were "aggravated" by failure to timely disclose breaches in the company's financial filing for more than two and a half years. Claims in the complaint include breach of fiduciary duty, corporate waste and unjust enrichment.

Ken Rashbaum heads Barton LLP's Privacy and Cyber-Security Practice. His team provides counsel on cyber-security assessments and cyber-security insurance coverage, drafts required policies and procedures and training materials and delivers cyber-security workforce training. The firm also represents organizations subject to an SEC cyber-security audit. Ken's bio is available at www.bartonesq.com/attorneys/kenneth-rashbaum/.



If you have any questions regarding the contents of this publication, please contact:

Kenneth Rashbaum

P: +1 212.885.8836
krashbaum@bartonesq.com