# Client Update

# SEC Sanctions Investment Adviser for Failing to Adopt Cybersecurity Policies and Procedures

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com

Michael P. Harrell
mpharrell@debevoise.com

Jim Pastore
jjpastore@debevoise.com

David Sarratt
dsarratt@debevoise.com

Derek Wikstrom
dwikstrom@debevoise.com

WASHINGTON, D.C.
Kenneth J. Berman
kjberman@debevoise.com

Jeffrey P. Cunard
jpcunard@debevoise.com

David A. O'Neil
daoneil@debevoise.com

In a recently disclosed action, the Securities and Exchange Commission ("SEC") found a registered investment adviser, R.T. Jones Capital Equities Management, Inc. (the "Adviser"), liable for failing to adopt written policies and procedures designed to protect customer records and information. (A copy of the Order is available here.) This Order makes good on the promises embodied in the SEC Division of Investment Management's April 2015 IM Guidance and the SEC Office of Compliance Inspections and Examinations ("OCIE") Cybersecurity Examination Guidelines issued earlier this month that the SEC will continue to focus on firms' development of robust cybersecurity protections. This case highlights the importance of the recommendations outlined at the end of this Client Update.

## BACKGROUND

The Adviser offered investment advice to participants in a retirement plan through a managed account program called Artesys. In order to confirm prospective clients' eligibility to enroll in the program, the Adviser would request their names, dates of birth, and social security numbers. The company would then check that information against a database it maintained containing the same personally identifiable information ("PII") from each of the more than 100,000 eligible participants. This database was stored, unencrypted, on a third-party-hosted web server.

In July 2013, the Adviser discovered a potential breach of that server. It did not have written cybersecurity policies or an incident response plan in place, but it promptly retained cybersecurity consultants, who were able to confirm that an intruder had gained full access and rights to copy the information in the database. Although the consultants couldn't determine whether the client data had actually been accessed, exfiltrated, or otherwise compromised during the breach, the Adviser provided notice, and free identity theft monitoring, to all

clients whose data may have been compromised. (To date, no client has reported suffering financial harm from the incident.)

## THE SEC'S FINDINGS

The SEC found that these facts represented a willful violation of Rule 30(a) of Regulation S-P, 17 C.F.R. § 248.30(a), which requires broker-dealers and investment advisers to maintain written policies and procedures to safeguard customer records and information.

The SEC censured the Adviser, ordered it to cease and desist from any continuing or future violations of the Regulation, and fined it $75,000. The Order notes that the company cooperated with the government and promptly took remedial steps including appointment of an information security manager, retention of a cybersecurity firm to provide reports and advice, implementation of a written information security policy, and elimination of the data security flaws that contributed to the breach.

This case serves as a useful reminder that registered investment advisers should carefully consider how to adopt the measures to address cybersecurity risks recommended by the SEC's Division of Investment Management in guidance issued in April of this year. That guidance instructed funds and advisers to establish strategies — memorialized in written policies and procedures — for preventing, detecting, and responding to cybersecurity threats.

## RECOMMENDATIONS

The Order points up the risks of disregarding the SEC's expectation that firms develop and continually refresh written policies and procedures for dealing with cybersecurity incidents. Firms should consider taking the following steps to protect themselves:

- Develop, test, and regularly update a formal, written Incident Response Plan. Ideally, this IRP should be distinct from any business continuity plans.
- Adopt and follow written cybersecurity policies and procedures.
- Engage outside counsel and consultants experienced with cybersecurity issues to assist in complying with the SEC's guidance.
- Develop and implement document and data retention policies. Prune data in accordance with those policies. Hackers can't steal what you don't have.

- Mind your third-party vendors. Consider contractual provisions that mandate a certain level of cybersecurity controls, appropriate indemnifications, and obligations to notify you in the event of a breach.
- Consistent with business needs, consider where encryption can be deployed to protect sensitive data.

This enforcement action continues the regulatory trend of converting technology "best practices" (e.g., encrypting sensitive data) into legally mandated requirements for managing cyber risk. It also underscores that regulators tend to borrow from each other in crafting mandates and guidance about cybersecurity, with the SEC joining Massachusetts and the Federal Financial Institutions Examination Council in calling on companies to develop written information security policies. All companies — regardless of whether they are SEC filers — would do well to consider the SEC's enforcement action in crafting their own data security programs. As the SEC and other government agencies increasingly focus on cybersecurity issues, companies must as well; the failure to do so may carry with it the consequences of an enforcement action.

* * *

Please do not hesitate to contact us with any questions.