UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

INVESTMENT ADVISERS ACT OF 1940
Release No. 4204 / September 22, 2015

ADMINISTRATIVE PROCEEDING
File No. 3-16827

In the Matter of

R.T. Jones Capital Equities Management, Inc.,

Respondent.

ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTIONS 203(e) AND 203(k) OF THE INVESTMENT ADVISERS ACT OF 1940, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASE-AND-DESIST ORDER

I.

The Securities and Exchange Commission ("Commission") deems it appropriate and in the public interest that public administrative and cease-and-desist proceedings be, and hereby are, instituted pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940 ("Advisers Act") against R.T. Jones Capital Equities Management, Inc. ("R.T. Jones" or "Respondent").

II.

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. Solely for the purpose of these proceedings and any other proceedings brought by or on behalf of the Commission, or to which the Commission is a party, and without admitting or denying the findings herein, except as to the Commission's jurisdiction over it and the subject matter of these proceedings, which are admitted, Respondent consents to the entry of this Order Instituting Administrative and Cease-and-Desist Proceedings Pursuant to Sections 203(e) and 203(k) of the Investment Advisers Act of 1940, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order ("Order"), as set forth below.

III.

On the basis of this Order and Respondent's Offer, the Commission finds that

Summary

These proceedings arise out of R.T. Jones's failure to adopt written policies and procedures reasonably designed to protect customer records and information, in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (the "Safeguards Rule"). From at least September 2009 through July 2013, R.T. Jones stored sensitive personally identifiable information ("PII") of clients and other persons on its third party-hosted web server without adopting written policies and procedures regarding the security and confidentiality of that information and the protection of that information from anticipated threats or unauthorized access. In July 2013, the firm's web server was attacked by an unauthorized, unknown intruder, who gained access rights and copy rights to the data on the server. As a result of the attack, the PII of more than 100,000 individuals, including thousands of R.T. Jones's clients, was rendered vulnerable to theft.

Respondent

1. R.T. Jones, located in St. Louis, Missouri, is an investment adviser registered with the Commission that has approximately 8400 client accounts and about $480 million in regulatory assets under management. The firm does not have custody of client assets.

Background

2. Through agreements with a retirement plan administrator and various retirement plan sponsors, R.T. Jones provides investment advice to individual plan participants using a managed account option called Artesys. Artesys offers a variety of model portfolios that range in investment objectives and risk profiles. Plan participants can access the Artesys program through R.T. Jones's public website. Plan participants who elect to enroll in the program are instructed to fill out a questionnaire on the website regarding their investment objectives and risk tolerance. Based on information provided in the questionnaire, R.T. Jones recommends a particular portfolio allocation from among the Artesys models to the client. If the client agrees to the recommended allocation, R.T. Jones provides trade instructions to the retirement plan administrator, which then effects the transactions. R.T. Jones does not control or maintain client accounts or client account information.

3. During the relevant period, in order to verify eligibility to enroll in Artesys, R.T. Jones required prospective clients to log on to its website by entering their name, date of birth and social security number. The login information was then compared against the PII of eligible plan participants, which was provided to R.T. Jones by its plan sponsor partners. R.T. Jones stored this PII, without modification or encryption, on its third party-hosted web server. To facilitate the verification process, the plan sponsors provided R.T. Jones with information about all of their plan participants. Thus, even though R.T. Jones had fewer than 8000 plan participant clients, its web server contained the PII of over 100,000 individuals.

4. R.T. Jones limited access to the PII stored on the server to two individuals who held administrator status. In July 2013, R.T. Jones discovered a potential cybersecurity breach at its third party-hosted web server. R.T. Jones promptly retained more than one cybersecurity consulting firm to confirm the attack and assess the scope of the breach. One of the forensic cybersecurity firms reported that the cyberattack had been launched from multiple IP addresses, all of which traced back to mainland China, and that the intruder had gained full access rights and copy rights to the data stored on the server. However, the cybersecurity firms could not determine the full nature or extent of the breach because the intruder had destroyed the log files surrounding the period of the intruder's activity.

5. Soon thereafter, R.T. Jones retained another cybersecurity firm to review the initial report and independently assess the scope of the breach. Ultimately, the cybersecurity firms could not determine whether the PII stored on the server had been accessed or compromised during the breach.

6. Shortly after the breach incident, R.T. Jones provided notice of the breach to all of the individuals whose PII may have been compromised and offered them free identity monitoring through a third-party provider. To date, the firm has not learned of any information indicating that a client has suffered any financial harm as a result of the cyber attack.

R.T. Jones Failed to Adopt Written Policies and Procedures Reasonably Designed to Safeguard Customer Information

7. The Safeguards Rule, which the Commission adopted in 2000, requires that every investment adviser registered with the Commission adopt policies and procedures reasonably designed to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer. The Commission adopted amendments to the Safeguards Rule, effective January 2005, to require that the policies and procedures adopted thereunder be in writing.

8. During the relevant period, R.T. Jones maintained client PII on its third party-hosted web server. However, the firm failed to adopt any written policies and procedures reasonably designed to safeguard its clients' PII as required by the Safeguards Rule. R.T. Jones's policies and procedures for protecting its clients' information did not include, for example: conducting periodic risk assessments, employing a firewall to protect the web server containing client PII, encrypting client PII stored on that server, or establishing procedures for responding to a cybersecurity incident. Taken as a whole, R.T. Jones's policies and procedures for protecting customer records and information were not reasonable to safeguard customer information.

Violations of the Federal Securities Laws

9. As a result of the conduct described above, R.T. Jones willfully[1] violated Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)), which requires registered investment advisers to adopt written policies and procedures that are reasonably designed to safeguard customer records and information.

Remedial Efforts

10. To mitigate against any future risk of cyber threats, R.T. Jones has appointed an information security manager to oversee data security and protection of PII, and adopted and implemented a written information security policy. Among other things, the firm no longer stores PII on its webserver and any PII stored on its internal network is encrypted. The firm has also installed a new firewall and logging system to prevent and detect malicious incursions. Finally, R.T. Jones has retained a cybersecurity firm to provide ongoing reports and advice on the firm's information technology security.

11. In determining to accept R.T. Jones's Offer, the Commission considered the remedial acts promptly undertaken by R.T. Jones and the cooperation R.T. Jones afforded the Commission staff.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in R.T. Jones's Offer. Accordingly, pursuant to Sections 203(e) and 203(k) of the Advisers Act, it is hereby ORDERED that:

A. Respondent R.T. Jones cease and desist from committing or causing any violations and any future violations of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a));

B. Respondent R.T. Jones is censured; and

C. Respondent R.T. Jones shall pay, within 10 (ten) days of the entry of this Order, a civil money penalty in the amount of $75,000 to the Securities and Exchange Commission. If timely payment is not made, additional interest shall accrue pursuant to 31 U.S.C. § 3717. Payment must be made in one of the following ways:

(1) Respondent may transmit payment electronically to the Commission, which will provide detailed ACH transfer/Fedwire instructions upon request;

[1] A willful violation of the securities laws means merely "'that the person charged with the duty knows what he is doing.'" *Wonsover v. SEC*, 205 F.3d 408, 414 (D.C. Cir. 2000) (quoting *Hughes v. SEC*, 174 F.2d 969, 977 (D.C. Cir. 1949)). There is no requirement that the actor "'also be aware that he is violating one of the Rules or Acts.'" *Id.* (quoting *Gearhart & Otis, Inc. v. SEC*, 348 F.2d 798, 803 (D.C. Cir. 1965)).

(2) Respondent may make direct payment from a bank account via Pay.gov through the SEC website at http://www.sec.gov/about/offices/ofm.htm; or

(3) Respondent may pay by certified check, bank cashier's check, or United States postal money order, made payable to the Securities and Exchange Commission and hand-delivered or mailed to:

Enterprise Services Center
Accounts Receivable Branch
HQ Bldg., Room 181, AMZ-341
6500 South MacArthur Boulevard
Oklahoma City, OK 73169

Payments by check or money order must be accompanied by a cover letter identifying R.T. Jones as a Respondent in these proceedings, and the file number of these proceedings; a copy of the cover letter and check or money order must be sent to: Paul Montoya, Assistant Regional Director, Asset Management Unit, Chicago Regional Office, Securities and Exchange Commission, 175 W. Jackson Blvd., Suite 900, Chicago, Illinois, 60604.

By the Commission.

Brent J. Fields
Secretary