Weil

Private Equity Alert

Did the Regulatory Cybersecurity Shoe Just Drop?

The SEC Enforcement Action in *In re R.T. Jones Capital Equities Management, Inc.*

By David Wohl and Paul Ferrillo

Just days after the SEC's Office of Compliance Inspections and Examinations ("OCIE") issued its second round of cybersecurity guidance for its upcoming examinations of registered investment advisers and broker-dealers,[1] the SEC settled an administrative proceeding on cybersecurity issues arising out of a breach at a registered investment adviser, R.T. Jones Capital Equities Management, Inc. ("R.T. Jones").[2] As a result of the settlement, R.T. Jones was censured and fined $75,000. On the heels of the recent OCIE guidance and following a year of major cybersecurity breaches (especially at financial institutions),[3] this proceeding is instructive on a number of points, especially on the question "What happens when you don't adopt policies and procedures to safeguard client data?"

The facts of the case are not complex. R.T. Jones provides portfolio allocation advice to retirement plan participants. To enroll participants, R.T. Jones collected personal information like names, dates of birth and social security numbers (termed "personally identifiable information" or "PII"). The PII was kept on a third party web server (we presume a cloud service provider or co-location information management company). In July 2013 R.T. Jones discovered it had been potentially breached at the third party server. R.T. Jones quickly hired a cyber forensic firm to investigate, but the firm ultimately could not determine the full extent of the breach because the cyber-attacker had destroyed the log files during the period it was moving laterally on the server. Another forensic firm was hired, and it too was unable to determine whether the PII stored on the server was accessed or compromised. Soon after discovery, R.T. Jones provided notice of the breach to all individuals whose PII may have been compromised, and to date there is no indication that any client has suffered financial harm as a result of the attack.

In its enforcement action, the SEC alleged that R.T. Jones willfully violated Rule 30(a) of Regulation S-P (the "Safeguards Rule"), which requires a registered investment adviser to adopt written policies and procedures that are reasonably designed to safeguard customer records and information. Specifically, the SEC found that R.T. Jones:

> "… 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."

What the R.T. Jones Proceeding Means for the Future

It appears that the potential breach at R.T. Jones pre-dated the cybersecurity guidance issued to date by both OCIE and the Financial Industry Regulatory Authority ("FINRA"). Given the unknown (if any) harm to clients, and the steps R.T. Jones took post-breach to greatly improve its cybersecurity posture (*e.g.*, appointing an information security manager, implementing written information security policies and procedures and hiring a cybersecurity firm to provide ongoing reports and advice on information technology security), it is plausible to conclude that the SEC felt greater sanctions were not warranted.

Juxtapose these (or perhaps worse) facts with today's regulatory environment, plus the abundant cybersecurity guidance recently issued by both OCIE and FINRA. Further suppose that there was provable monetary damage to clients as a result of a breach. What if a firm has not taken any remediation efforts even though cybersecurity weaknesses have been identified by a regulatory examination? In those cases, it is likely the SEC or another regulator would seek a much larger penalty than the one levied on R.T. Jones.

The R.T. Jones proceeding shows that cybersecurity regulators (whether the SEC, FINRA, the Federal Trade Commission or the Federal Financial Institutions Examination Council) are watching closely. OCIE has issued two rounds of guidance, and OCIE and FINRA have already conducted one round of examinations, with another OCIE exam initiative coming up. In light of these developments, now is a good time for firms to review previous guidance and compare it to their existing cybersecurity policies and procedures. If there is a gap, that is a bad thing. If there are many gaps, even worse. But with proper assistance, required policies and procedures can be adopted, incident response and compromise assessments can be performed, and regulated entities can show examiners that "they are not R.T. Jones."

---

1. See OCIE's 2015 Cybersecurity Examination Initiative, available at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf; "OCIE Publishes Risk Alert Regarding Cybersecurity Examination Initiative for Registered Investment Advisers and Broker-Dealers," available at http://www.weil.com/~/media/publications/private-equity-alert/pe_alert_sep_015.pdf.
2. The R.T. Jones settlement is available at http://www.sec.gov/litigation/admin/2015/ia-4204.pdf.
3. See "Hacking the Street? FIN4 Likely Playing the Market," available at https://www2.fireeye.com/fin4.html.

Private Equity Alert is published by the Private Equity practice group of Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

The Private Equity group's practice includes the formation of private equity funds and the execution of domestic and cross-border acquisition and investment transactions. Our fund formation practice includes the representation of private equity fund sponsors in organizing a wide variety of private equity funds, including buyout, venture capital, distressed debt, and real estate opportunity funds, and the representation of large institutional investors making investments in those funds. Our transaction execution practice includes the representation of private equity fund sponsors and their portfolio companies in a broad range of transactions, including leveraged buyouts, merger and acquisition transactions, strategic investments, recapitalizations, minority equity investments, distressed investments, venture capital investments, and restructurings.

If you have questions concerning the contents of this issue, or would like more information about Weil's Private Equity practice group, please speak to your regular contact at Weil, or to the editors, practice group leaders or contributing authors:

Authors:

Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372
David Wohl (NY)	Bio Page	david.wohl@weil.com	+1 212 310 8933