SEC settlement informed by cyber security guidelines

On 22 September, the US Securities and Exchange Commission ('SEC') announced that R.T. Jones agreed to settle charges that it "willfully" 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 reasonably designed to safeguard customer records and information. The predicate for the violation was that R.T. Jones had failed to establish cyber security policies and procedures to safeguard personally identifiable information ('PII'). A breach of the systems that held client PII was feared potentially to have compromised the PII of tens of thousands of individuals. Cyrus Amir-Mokri, Stuart D. Levi and Anastasia T. Rockas of Skadden provide detailed analysis of the case and the guidelines to be followed.

The *R.T. Jones* case helps clarify some questions around regulatory and enforcement expectations of the financial regulatory community with respect to cyber security. In particular, two themes emerge from the SEC's discussion of the case[1]. First, although the cyber security guidelines issued by regulators are not binding, the regulators may rely on those guidelines to inform their enforcement decisions. Second, when adopting cyber security measures, companies should take a holistic approach that incorporates both preparedness and incident response protocols.

The significance of guidelines

In the past two years, the financial regulators' pronouncements in this area has consisted largely of guidelines that outline steps companies should consider taking to enhance their cyber security. Indeed, the SEC's Division of Investment Management issued cyber security guidelines along these lines in April 2015[2]. These guidelines, including those issued by the SEC's Division of Investment Management, are largely based on the National Institute of Standards and Technology Cybersecurity Framework ('NIST Framework')[3]. They outline a framework for cyber security preparedness and incident response.

Just like the NIST standards, the regulatory guidelines do not purport to be hard-wired requirements, but general principles to assist firms with fashioning a cyber security programme. That said, the *R.T. Jones* case illustrates one way in which such guidelines can inform enforcement actions. Although the guidelines do not form the basis for asserting an enforcement action - the guidelines can help provide standards of conduct that regulators and enforcement authorities may use to determine when a culpable breach of a binding rule has taken place.

Take the regulation at issue in the *R.T. Jones* case. The SEC's order does not base assertions of violation on the cyber security guidelines, but finds that R.T. Jones violated Rule 30(a) of Regulation S-P under the Securities Act of 1933. This so-called 'Safeguards Rule' was adopted by the SEC in 2000 under the authority of Section 504 of the Gramm-Leach-Bliley Act[4]. The rule requires SEC-registered investment advisers to adopt policies and procedures reasonably designed to: (1) protect 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 unauthorised access to or use of customer records or information that could result in substantial harm or inconvenience to any customer[5]. Effective in 2005, the SEC added the requirement that the policies and procedures under the rule be in writing.

In explaining why the defendant in the *R.T. Jones* matter had violated the Safeguards Rule, the SEC's Enforcement Division stated that the firm "failed entirely to adopt written policies and procedures reasonably designed to safeguard customer information," adding that "R.T. Jones failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cybersecurity incidents."[6] Thus, the Enforcement Division appears not only to be faulting R.T. Jones for a failure to have written policies and procedures, but also to be suggesting that specific measures - ranging from risk assessments to ways of isolating core assets and protocols for incident response - should be a part of those policies and procedures. The latter measures are outlined in guidelines such as the NIST Framework and the Division of Investment Management's 2015 guidance.

The interconnection between specific data protection rules and cyber security guidelines had been alluded to by FINRA in its report on cyber security measures and practices[7]. In that report, FINRA cites Regulation S-P and explains that, as broker-dealers perform cyber risk assessments to determine critical assets, "one consideration in identifying critical assets is firms' obligations under Regulation S-P to protect customers' personally identifiable information (PII)." The

implication being that obligations under Regulation S-P could be evaluated with reference to prevailing cyber security guidelines concerning cyber risk assessments.

Examples of this interconnection are not limited to preparedness. The FINRA report indicates, for example, that poor incident response could also provide a basis for enforcement action. The report states that during an incident, "firms are expected to conduct a timely investigation of the incident to determine the extent of data or monetary loss and identify root causes." It adds that "[t]he failure to conduct an adequate investigation of a breach has been a contributing factor to an enforcement action." In another FINRA enforcement matter, "one factor cited in the settlement was a firm's failure to rapidly remediate a device the firm knew was exposing customer information to unauthorized users."

Incident response plans should have provisions for notification and reporting. The FINRA report draws explicit links between SEC regulations and incident response practices. The report states that an incident response plan "should identify the parties to be notified, as well as what information should be reported and when," adding that "[f]irms may have notification obligations pursuant to, for example, Regulation S-ID, state reporting requirements and FINRA rules." The report also notes that firms have reporting obligations under FINRA Rule 4530(b) and urges firms to report material cyber incidents that do not trigger a reporting obligation to their regulatory coordinator.

A holistic approach

The second lesson to be drawn is that, when adopting a cyber security framework and plan of action, it is important to adopt the entire framework. Preparedness without adequate incident response is not enough; similarly, expending efforts to manage an incident will not immunise a firm to regulatory or enforcement action if preparedness is lacking.

Preparedness without adequate incident response is not enough; similarly, expending efforts to manage an incident will not immunise a firm to regulatory or enforcement action if preparedness is lacking

Based on the settlement, it appears that R.T. Jones expended significant efforts in managing an expeditious and effective incident response. According to the settlement document, once R.T. Jones discovered a potential breach at its third party hosted web server in July 2013, it "promptly retained more than one cybersecurity consulting firm to confirm the attack and assess the scope of the breach."[8] The perpetrators appear to have been sophisticated, as one of the cyber security firms reported that the attack had been traced to multiple IP addresses, all from China. Although the attackers had gained full access to the data, the cyber security firms could not determine the full nature or extent of the breach because the attackers had destroyed the log files. What is more, although the cyber security firms had established the fact of a breach, they could not determine whether PII had been accessed or compromised.

Even so, R.T. Jones provided notice of the breach to all individuals whose PII may have been compromised and offered them free identity monitoring. The settlement agreement states that, "[t]o 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." Once the breach was discovered, R.T. Jones expended substantial resources and efforts in managing the incident, which included trying to establish the source and seeing to it that customers were notified and protected. But still these actions were not sufficient to prevent an enforcement action grounded on an *ex ante* lack of preparedness.

Firms should ensure that they have cyber security policies and procedures, and that these are written. Moreover, the policies and procedures should cover not only incident response, but also preparedness. That is, even in the absence of an incident, firms should have policies and procedures to identify their critical assets, evaluate the risk of breach to critical assets, isolate the core critical assets through firewalls or encryption, keep updated on threat information, ensure that the most recent defences and patches are applied, stress testing is being performed, and so on. The regulators' guidelines are a helpful source for the kinds of steps that should be taken in this regard.

Even taking all of these steps, of course, does not guarantee that a breach will not occur. But if there is a breach, having taken those steps will provide a basis to defend against charges that the company unreasonably failed to adopt policies and procedures for protecting PII.

Cyrus Amir-Mokri Partner
Stuart D. Levi Partner
Anastasia T. Rockas Partner
Skadden, New York
cyrus.amir-mokri@skadden.com

1. R.T. Jones Capital Management, Inc., File No. 3-16827, SEC Release No. 4204 (22 Sept 2015), https://www.sec.gov/litigation/admin/2015/ia-4204.pdf
2. US SEC, Division of Investment Management, Guidance Update: Cybersecurity Guidance, No. 2015-02 (April 2015).
3. NIST, Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0, 12 Feb 2014).
4. 15 U.S.C. §6804.
5. 17 C.F.R. §248.30.
6. SEC, Press Release 2015-202 (Sep 22, 2015), http://www.sec.gov/news/pressrelease/2015-202.html
7. FINRA, Report on Cybersecurity Practices (Feb 2015).
8. R.T. Jones Capital Management, SEC Release No. 4204 at 3.