Hedge Fund Law Report
An Acuris company

Cybersecurity

Business Emails Must Be Secure to Avoid SEC Enforcement Action

May 12, 2016

By Rebecca Hughes Parker, *Hedge Fund Law Report*

As it continues to enforce appropriate cybersecurity controls, the SEC initiated administrative proceedings against Craig Scott Capital (CSC), a broker-dealer based in Uniondale, New York, and its two principals for failing to protect confidential consumer information by using personal email addresses for business matters. "The enforcement action, including the fines imposed, reflects how seriously the SEC takes the adoption of and compliance with proper policies and procedures," Anastasia Rockas, a partner at Skadden, told the Hedge Fund Law Report.

This enforcement action is particularly relevant to any hedge fund manager that: has an in-house broker-dealer; has high net worth individuals as clients; manages alternative mutual funds and thus has retail investors; or is subject to any look-through of its institutional clients to underlying individual investors. However, all hedge fund managers should pay close attention given that, as Rockas noted, the "SEC has indicated there will be additional enforcement actions in this space and has designated cybersecurity as an examination priority for 2016. The agency began a second round of examinations specifically focused on cybersecurity issues as announced by OCIE in September of 2015." See "OCIE Risk Alert Provides Cybersecurity Guidance to Investment Advisers and Broker-Dealers" (Sep. 24, 2015).

She stressed that companies should be monitoring their policies and procedures regularly for compliance and should have "appropriate technology in place to safeguard networks and non-public information." See "How Financial Service Providers Can Address Common Cybersecurity Threats," Cybersecurity Law Report (Mar. 16, 2016).

CSC's Cybersecurity Compliance Problems

CSC's Failure to Properly Handle Faxes

In the Cease and Desist Order (containing allegations that CSC has neither admitted nor denied), the SEC alleged that, after CSC was approved for membership in FINRA on January 20, 2012, the company set up email addresses for all employees with the @craigscottcapital.com domain name and used a third-party service provider to archive email to comply with SEC rules. The provider archived only emails with that email suffix.

From January 2012 to June 2014 (which the SEC defines as the Relevant Period), CSC used an eFax system to convert faxes to emails. Two of the emails CSC set up to receive eFaxes were non-business email addresses, including the personal address of an administrative assistant.

Thus, according to the SEC, many eFaxes were not properly archived. These eFaxes routinely contained customer records and information such as social security numbers, birth dates, account numbers, driver's licenses and copies of checks.

Though CSC's chief compliance officer (CCO) determined in June 2013 that the delivery of the eFaxes to a non-business email address was a problem and set up a new email address, fax@craigscottcapital.com, eFaxes going to one personal email address were not routed to the new address until October 1, 2013, and emails were still being sent to the second non-firm email address until May 22, 2014.

CSC's Use of Personal Email for Business Purposes

The SEC also alleged that CSC principals and employees used non-firm email addresses for communications with third parties as well as for internal discussions. These emails – 25,000 during the Relevant Period – contained consumer information similar to the eFaxes. The SEC also noted that when the two principals of CSC implicated in this matter – Craig Taddonio and Brent Porges – used the personal emails, they included signature blocks with their CSC contact information.

This was in contravention of CSC's written supervisory procedures (WSPs), which prohibited the use of personal email for business purposes.

Blank Spaces in the Safeguards Rule Policy

The SEC alleged further that CSC failed to maintain policies and procedures reasonably designed to safeguard client information in violation of Rule 30(a) of Regulation S-P (17 C.F.R. § 248.30(a)) (Safeguards Rule), which requires that every investment adviser registered with the SEC adopt policies and procedures reasonably designed to:

1. ensure 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 rule was amended in 2005 to require that the policies and procedures be in writing. See "K&L Gates-IAA Panel Addresses Regulatory Compliance and Practical Elements of Cybersecurity Testing (Part Two of Two)" (May 28, 2015).

According to the SEC, the Safeguards Rule Policy portion of CSC's WSPs lacked several crucial pieces of information:

1. Though the Safeguards Rule Policy stated that the "Designated Supervisor" was responsible for ensuring compliance with the policy, it did not identify the Designated Supervisor;
2. Though CSC used an eFax System, which received emails to non-firm email addresses, the Safeguards Rule Policy did not address either the eFax System or how to handle customer records and information contained in eFaxes; and
3. The Safeguards Rule Policy contained blanks to be filled in later, such as: "[The Firm] has adopted procedures to protect customer information, including the following: [methods]."

Further, the SEC said that CSC did not follow what was written in the Safeguards Rule Policy. For example, the policy stated that customer records and information may be accessed outside of the office by employees who received approval from CSC's designated information officer and who have appropriate firewalls on their devices. However, there was no designated information officer, and the employees who accessed customer records and information did not have the appropriate firewall. The Safeguards Rule Policy also required the encryption of customer records and information transmitted to laptops and devices, but the SEC said that this encryption never occurred.

The Penalties

The SEC said that CSC willfully violated the Safeguards Rule, as well as Section 17(a) of the Securities Exchange Act of 1934 and Rule 17a-4(b)(4) thereunder. The latter rules require that brokers or dealers make and keep current various records relating to their business and preserve those records for three years.

The charges against Taddonio and Porges include willfully aiding and abetting and causing CSC's violations of Section 17(a) and Rule 17a-4(b)(4).

The SEC ordered all of the defendants to cease and desist from violating the relevant laws and censured them. CSC was ordered to pay $100,000, and the defendants $25,000 each.

"Compliance officers and senior management who are responsible for supervising policies and procedures, but who are instead involved in the violations, may be held personally responsible," Rockas warned. For more on CCO liability, see "SEC Enforcement Director Assures CCOs They Need Not Fear SEC Action Absent Wrongdoing" (Nov. 19, 2015); "SEC Commissioner Speaks Out Against Trend Toward Strict Liability for Compliance Personnel" (Jun. 25, 2015); and "SEC Commissioner Issues Statement Supporting Hedge Fund Manager Chief Compliance Officers" (Jul. 16, 2015).

The Enforcement Landscape

R.T. Jones: A Hack, No Harm and a Lesser Fine

This action follows on the heels of an action the SEC took against R.T. Jones Capital Equities Management, Inc. (R.T. Jones). There "was no finding of harm in either" the R.T. Jones or the CSC case, Rockas said, "but in R.T. Jones there also was a cybersecurity breach resulting in the disclosure of personally identifiable information relating to approximately 100,000 individuals, including firm clients."

R.T. Jones kept a large amount of personally identifiable information (PII) on a web-based third-party server without encryption. The server was hacked. R.T. Jones notified all individuals whose PII may have been compromised and provided each with third-party identity theft monitoring. The SEC issued a civil monetary penalty of $75,000 in the September 22, 2015, Cease-and-Desist Order. See "Investment Adviser Penalized for Weak Cyber Policies; OCIE Issues Investor Alert" (Oct. 1, 2015).

The September 2015 Investor Alert

The SEC has issued a few documents that telegraph its enforcement priorities in this space. At the same time it announced the R.T. Jones case, the SEC issued an Investor Alert reminding companies of the steps they should take if PII has been compromised or stolen. Steps include closing accounts, using two-step verification, placing fraud alerts with a credit bureau and creating an Identity Theft Report.

"Investment advisers should ensure that their policies address the issues outlined by the SEC in its guidance updates and that policies and procedures are specifically tailored to their businesses and perceived risks," Rockas said.

The April 2015 Investment Management Guidance

Rockas cited the April 2015 IM Guidance as helpful for firms. In that guidance, the SEC recommended that firms periodically have their cybersecurity assessments performed by experts and that they create a cybersecurity strategy that includes such measures as controlling access to various systems, encrypting data, restricting the use of removable storage media and developing an incident response plan. The IM Guidance also stresses that companies should have written policies and procedures and adequate training on those policies and procedures. See "SEC Guidance Update Suggests a Three-Step Framework for Investment Manager Cybersecurity Programs" (May 7, 2015).

Cybersecurity Examination Initiatives

"The two cybersecurity examination initiatives announced by OCIE in National Exam Program Risk Alerts also include helpful guidance," Rockas said.

OCIE indicated that the purpose of the September 2015 initiative – and the second round of examinations – is twofold: to build on the findings of its first round of exams and to address concerns that weak controls were implicated in certain recent cybersecurity breaches. The initiative enumerates six areas on which this exam initiative will focus and provides sample requests for information for each of those areas. OCIE noted that many of the information requests track the February 2014 "Framework for Improving Critical Infrastructure Cybersecurity," issued by the National Institute of Standards and Technology. See our two-part series covering the K&L Gates-IAA panel on cybersecurity for investment managers: "Laws and Threats" (Apr. 23, 2015); and "Risk Mitigation Frameworks and Techniques" (Apr. 30, 2015).

This material has been printed by and is for their consumption only. The full Terms of Use are available at www.hflawreport.com.
UNAUTHORIZED USE OR DISTRIBUTION IS UNLAWFUL