OCIE OBSERVATIONS FROM THE SECOND ROUND OF CYBERSECURITY EXAMINATIONS

Date: 17 August 2017

U.S. Investment Management Alert

By: Eden L. Rohrer, Jeremy M. McLaughlin, Julia B. Jacobson, Vincente L. Martinez, Robert M. Crea, Evan J. Glover

On August 7, 2017, the Securities and Exchange Commission's ("SEC") Office of Compliance Inspections and Examinations ("OCIE") released a risk alert (the "Risk Alert") summarizing observations from the second round of cybersecurity sweep examinations on 75 SEC registered investment firms including broker-dealers, investment advisers, and investment companies.

OCIE announced its first cybersecurity sweep initiative in April 2014 and shortly thereafter conducted an initial sweep examination of 57 broker-dealers and 49 investment advisers. In September 2015, OCIE announced that a second round of examinations would focus on firms' written policies and procedures and assessing the implementation of those polices and procedures, specifically: (1) governance and risk assessment; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response. The second round initiative also included a different population of firms, and unlike the first round also included investment companies.

In both initiatives, OCIE announced the sweeps through risk alerts and in both instances OCIE attached to those risk alerts Appendices, which contained lists of questions and topics that registrants could expect to encounter in an SEC cybersecurity examination. The risk alerts announcing the first round and second round of sweep examinations should be considered essential reading. K&L Gates issued the following client alerts on the SEC's takeaways from the first round and the announcement of the second round, which may be found here and here.

SEC OBSERVATIONS

On the positive side, the Risk Alert noted a general improvement in cybersecurity preparedness since the first round. However, areas pertaining to oversight and compliance could still be improved to address existing vulnerabilities.

The Risk Alert included the following observations:

- The vast majority of investment advisers and funds, and nearly all broker-dealers conducted periodic risk assessments to identify cybersecurity threats and vulnerabilities, in addition to potential business consequences of a cyber incident;

- Despite the fact that nearly all broker-dealers and almost half of the advisers and funds conducted vulnerability scans and penetration tests on critical firm systems, firms did not appear to fully remediate some high-risk observations discovered by the tests and scans;
- All firms had some tool or system to prevent, detect, and monitor personal identification information data loss;
- Although all broker-dealers and nearly all advisers and funds had a regular system maintenance process in place (including the installation of software patches), a few of the firms had a significant number of security patches (including critical system updates) that had not yet been installed;
- Nearly all firms had policies and procedures that addressed Regulation S-P and cyber-related business continuity plans, and most advisers and funds and nearly all broker-dealers had specific Regulation S-ID and cybersecurity policies;
- While the majority of broker-dealers had plans for data breach incidents and notifying clients of material events, less than two-thirds of the advisers and funds had such plans;
- All broker-dealers and a substantial number of advisers and funds either maintained a cybersecurity organizational chart and/or delineated cybersecurity roles and responsibilities within the firm;
- The vast majority of broker-dealers and two-thirds of advisers and funds had authority to transfer customer/shareholder funds to third-party accounts;
- While all of the advisers and funds maintained policies regarding the verification of customer identities to transfer funds, some broker-dealers appeared to have informal practices but did not memorialize their process into the firm's written supervisory procedures; and
- All firms either conducted vendor risk assessments or had vendors provide the firm with a risk management and performance report, in addition to certification reports or security reviews.

OCIE specifically observed that a majority of firms' information protection policies and procedures appeared to have one or more of the following issues:

1. Policies and procedures were not reasonably tailored to the firm's business;
2. Firms either did not adhere to the policies and procedures of the policies did not reflect actual practices of the firm; and
3. Firms that did not appear to adequately conduct system maintenance (i.e., firms were using outdated operating systems or failed to fully remediate discovered vulnerabilities) were also exposed to data breach vulnerabilities that could give rise to data privacy related issues arising under Regulation S-P.

During these examinations, OCIE staff observed six elements included in the policies and procedures of firms that OCIE believed had implemented robust controls. While not recommendations per se, the Risk Alert states that firms would benefit from considering such elements:

4. *Maintenance of an inventory of vendors, data, and information* - Policies and procedures included a complete inventory of data and information, along with classifications of the risks, vulnerabilities, data, business consequences, and information regarding each service provider and vendor, if applicable.

5. *Detailed cybersecurity-related instructions regarding items such as penetration test, security monitoring and system auditing, access rights, and reporting* - OCIE provided specific examples of how instructions were given with respect to penetration tests, security monitoring and system auditing, access rights and reporting.
6. *Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities* - Vulnerability scans of core IT infrastructure were required with prioritized action items for any identified concerns and patch management policies.
7. *Established and enforced controls to access systems and data* - Certain firms included detailed "acceptable use" policies specifying employees' obligations when using firm networks and equipment and also required and enforced controls for mobile devices. Third-party vendors were required to provide periodic logs of their activity on firms' networks. Immediate termination of access for terminated employees and very prompt termination of access for employees that left voluntarily.
8. *Mandatory employee training* - Information security training at on-boarding and periodically thereafter.
9. *Engaged senior management* - Management involved in vetting and approving applicable policies and procedures.

K&L TAKEAWAYS

For some years, OCIE has repeated the refrain that policies and procedures should be reasonably tailored, applied to the business, enforced, and periodically tested. The Risk Alert continues that trend by providing specific and detailed examples of how firms could implement and apply their cybersecurity policies and procedures. Among those recommendations is an emphasis that firms take steps to remediate discovered vulnerabilities.

OCIE points out in the Risk Alert that its views are those of the staff, that they do not constitute legal advice, and that the Commission itself has expressed no view on the contents of the Risk Alert. Further, Regulation S-P Rule 30(a)—which defines the standard of care for handling customer records and information—is a principles-based rule that does not contain specific technological requirements, but rather requires registrants to have policies and procedures "reasonably designed" to insure the security and confidentiality of customer records and information, to protect against anticipated threats, and to protect against unauthorized access. While those factors might lead registrants to conclude that OCIE's recommendations are not required, firms should act with caution. To the extent that OCIE clarifies its expectations through risk alerts, those expectations may become the standards against which the OCIE will judge a registrant's cybersecurity efforts, either in an examination or investigation. Registrants should consider carefully how closely their policies and procedures adhere to the guidance from OCIE, and whether departures from such guidance are defensible under the reasonable design standard.

OCIE, in conducting its cybersecurity examinations, will expect that firms be familiar with and have considered its guidance. We also have observed that OCIE has looked favorably on firms that incorporate guidance from specific industry standards, such as the National Institute of Standards and Technology or the International Organization for Standardization in their compliance policies and procedures. Such standards will not be applicable to every firm, but knowledge about such standards can prove helpful in tailoring and applying

appropriate policies and procedures. Any implementation of such standards should be handled in concert with a professional third-party consultant.

Additionally, beyond the SEC's cybersecurity regime, firms should be aware that they may be subject to requirements of other regulatory bodies. Specifically, some firms may be subject to requirements imposed by the Federal Trade Commission and the Financial Industry Regulatory Authority. Certain states also impose cybersecurity requirements. Such regulatory requirements may be above and beyond those of the SEC's.

Notes:

1. *See* 17 C.F.R. Part 248, Subpart A—Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information. *See also* Disposal of Consumer Report Information, Securities Exchange Act of 1934 ("Exchange Act") Release No. 50781, Investment Advisers Act of 1940 ("Advisers Act") Release No. 2332, Investment Company Act of 1940 ("Investment Company Act") Release No. 26685 (December 2, 2004), 69 Fed. Reg. 71321 (December 8, 2004) and Privacy of Consumer Financial Information (Regulation SP), Exchange Act Release No. 42974, Investment Company Act Release No. 4543, Advisers Act Release No. 1883 (June 22, 2000), 65 Fed. Reg. 40334 (June 29, 2000).

2. *See* Identity Theft Red Flags Rules, Exchange Act Release No. 69359, Advisers Act Release No. 3582, Investment Company Act Release No. 30456 (April 10, 2013), 78 Fed. Reg. 23637 (April 19, 2013). See 17 C.F.R. Part 248, Subpart C—Regulation S-ID: Identity Theft Red Flags.

3. OCIE also recommended that firms consider guidance from the SEC's Division of Investment Management and the cybersecurity issues discussed in Commission orders in settled enforcement proceedings. *See*, e.g., IM Guidance Update: Cybersecurity Guidance (April 2015), In re Morgan Stanley Smith Barney LLC, Exchange Act Release No. 78021, Advisers Act Release No. 4415 (June 8, 2016), In re R.T. Jones Capital Equities Management Inc., Advisers Act Release No. 4204 (September 22, 2015), and In re Craig Scott Capital LLC, Exchange Act Release No. 77595 (April 12, 2016).

KEY CONTACTS

EDEN L. ROHRER
PARTNER

NEW YORK
+1.212.536.4022
EDEN.ROHRER@KLGATES.COM

JEREMY M. MCLAUGHLIN
PARTNER

SAN FRANCISCO
+1.415.882.8230
JEREMY.MCLAUGHLIN@KLGATES.COM

