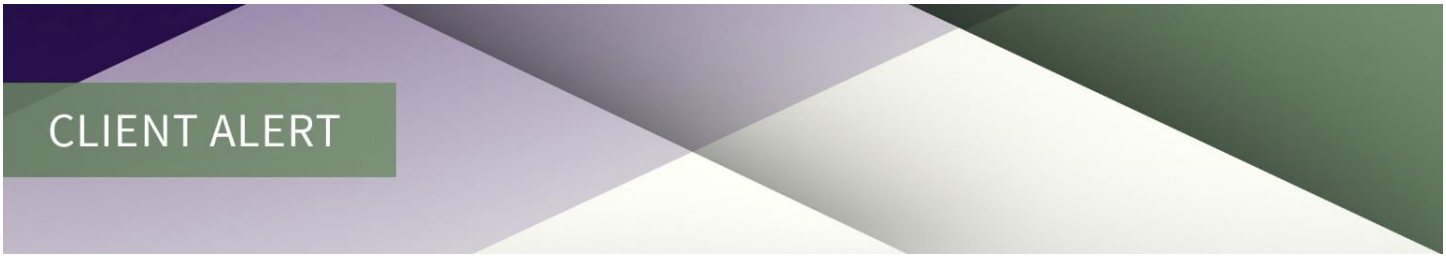
WILLKIE FARR & GALLAGHER LLP



SEC Staff Issues Guidance on Cloud Storage and Data Security for Broker-Dealers and Investment Advisers

June 7, 2019

AUTHORS

Daniel K. Alvarez | P. Georgia Bullitt | Justin L. Browder | Anne C. Choe
Elizabeth P. Gray | Marc J. Lederer

The Securities and Exchange Commission's (the "SEC") Office of Compliance Inspections and Examinations ("OCIE") published a risk alert on May 23, 2019 (the "May Risk Alert"),[1] offering its observations and guidance for broker-dealers and investment advisers ("Firms") on cloud storage and data security. This guidance is relevant for Firms that are subject to the Safeguards Rule of Regulation S-P[2] and the Identity Theft Red Flags Rule of Regulation S-ID.[3] The May Risk Alert reflected concepts articulated by Peter Driscoll, Director of OCIE, in a speech on Cybersecurity and Technology Controls[4] and a separate OCIE risk alert published on April 16, 2019, which provided other observations on compliance with

1 Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features, OCIE Risk Alert (May 23, 2019), *available at* May Risk Alert.

2 The Safeguards Rule of Regulation S-P requires every broker-dealer and investment adviser registered with the SEC to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. 17 C.F.R. 248.30(a).

3 The Identity Theft Red Flags Rule of Regulation S-ID requires broker-dealers and investment advisers registered or required to be registered with the SEC to develop and implement a written identity theft prevention program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. 17 C.F.R. 248.201.

4 Remarks at the SIFMA Operations Conference & Exhibition: Staying Vigilant to Protect Investors, Peter Driscoll (May 8, 2019).

Regulation S-P (the "April Risk Alert").[5] These communications emphasize that protecting retail investors by ensuring Firms have cybersecurity and technology controls in place continues to be and has been a top OCIE priority for several years. In the Risk Alerts and speech, OCIE reminds financial institutions that, as they move to cloud-based storage and utilize third-party technology providers, they need to include comprehensive vendor management as a component of the overall cybersecurity approach and to ensure proper security configuration management of network and cloud storage used for customer data. Earlier this year, OCIE included cybersecurity among its top six 2019 Examination Priorities. Continued cybersecurity examinations, which may be informed by these Risk Alerts, are expected.

In the May Risk Alert, OCIE focused on these themes and provided examples of effective practices regarding configuration of network storage solutions, oversight of vendors and updating of policies and procedures to reflect new types of storage solutions, including cloud-based storage. In particular, OCIE highlighted the following examples of deficiencies:

- Misconfigured network storage solutions: Firms did not adequately configure the security settings on their network storage solution to protect against unauthorized access. In addition, some Firms did not have policies and procedures addressing the security configuration of their network storage solution. Often, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially implemented. Examples of effective practices to address these issues include policies and procedures designed to support the initial installation, ongoing maintenance, and regular review of their network storage solution. Another example of an effective practice are guidelines for security controls and baseline security configuration standards to ensure that each network storage solution is configured properly.

- Inadequate oversight of vendor-provided network storage solutions: Firms did not ensure, through policies, procedures, contractual provisions, or otherwise, that the security settings on vendor-provided network storage solutions were configured in accordance with the Firm's security standards. An example of an effective practice to address are vendor management policies and procedures that include, among other things, regular implementation of software patches and hardware updates followed by reviews to ensure that such patches and updates did not unintentionally change, weaken, or otherwise modify the security configuration.

- Insufficient data classification policies and procedures: Firms' policies and procedures did not identify the different types of data stored electronically by the Firm nor the appropriate controls for each type of data.

[5] Investment Adviser and Broker-Dealer Compliance Issues Related to Regulation S-P – Privacy Notices and Safeguard Policies, OCIE Risk Alert (April 16, 2019), *available at* April Risk Alert.

In the May speech, OCIE Director Driscoll noted that OCIE staff members have identified security risks associated with storage of customer information in network storage solutions, including those leveraging cloud technology. These included the following:

- Missing coverage in policies and procedures: Firm policies and procedures did not address (and should address) standard security features, such as encryption, password protection and other tools designed to limit access, configurations to the security settings on storage solutions to protect against unauthorized access, and requirements for implementing secure configurations (especially in cloud storage).

- Hardware security: Firms should assess their policies and procedures for inventorying, deactivating and removing physical devices on their networks, as well as those designed to prevent the loss of sensitive data on such devices.

In the April Risk Alert, OCIE provided a number of observations in relation to data security and Regulation S-P.

- Personal devices: Firms' policies and procedures did not address how employee personal devices were to be properly configured to safeguard customer information.

- Electronic communications: Firms did not appear to have policies and procedures reasonably designed to prevent employees from regularly sending unencrypted emails to customers containing personally identifiable information ("PII").

- Training and monitoring: Employees were not provided adequate training on transmitting customer information via encrypted, password-protected and only Firm-approved methods, and Firms failed to monitor if the policies were being followed by employees.

- Unsecure networks: Firms' policies and procedures did not prohibit employees from sending customer PII to unsecure locations outside of the Firms' networks.

- Outside vendors: Firms failed to require outside vendors to contractually agree to keep customer PII confidential, even though such agreements were mandated by the Firm's policies and procedures.

- PII inventory: Firms' policies and procedures did not identify all systems on which the Firm maintained customer PII.

- Incident response plans: Written incident response plans did not address important areas, such as role assignments for implementing the plan, actions required to address a cybersecurity incident, and assessments of system vulnerabilities.

- Unsecure physical locations: Customer PII was stored in unsecure physical locations, such as in unlocked file cabinets in open offices.
- Login credentials: Customer login credentials had been disseminated to more employees than permitted under Firms' policies and procedures.
- Former employees: Former employees of Firms retained access rights after their departure and therefore could access restricted customer information.

The Risk Alerts emphasize the importance of policies, procedures and practices with respect to safeguarding customer information and initial and ongoing oversight of vendors that store or have access to electronic customer records, including cloud providers. We expect the SEC staff to continue to focus its examination efforts on cybersecurity, and we anticipate that the SEC may bring additional enforcement actions[6] against Firms for violations of Regulation S-P or Regulation S-ID.

[6] See here for our client alert on an SEC cybersecurity enforcement action.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

P. Georgia Bullitt
212 728 8250
gbullitt@willkie.com

Justin L. Browder
202 303 1264
jbrowder@willkie.com

Anne C. Choe
202 303 1285
achoe@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

Marc J. Lederer
212 728 8624
mlederer@willkie.com