LOS ANGELES
Daily Journal
www.dailyjournal.com
MONDAY, DECEMBER 8, 2014

PERSPECTIVE

A new wave of data privacy enforcement

By Kevin F. Cahill and D. Brett Kohlhofer

Cybersecurity risks are a growing issue for the financial sector — and regulators have taken notice. Earlier this year, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) announced in a Risk Alert that it would conduct examinations of over 50 registered broker-dealers and registered investment advisers, focusing on areas related to cybersecurity. In discussing the preliminary results of examinations conducted through September, OCIE's senior technology officer revealed that 87 percent of examined firms reported experiencing some form of "cyberincident." Examined firms ranked employee misconduct as among their top concerns.

It's no wonder that SEC Chair Mary Jo White has indicated that cybersecurity threats are "of extraordinary and long-term seriousness."

An Evolving Regulatory Mosaic

State and federal laws impose a patchwork of data privacy-related duties on broker-dealers and advisers. Regulation S-P provides that "[e]very broker, dealer, and investment company, and every investment adviser registered with the [SEC] must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." Regulation S-P requires that these be "reasonably designed" to (i) "[i]nsure the security and confidentiality of customer records and information"; (ii) "[p]rotect against any anticipated threats or hazards to the security or integrity of customer records and information"; and (iii) "[p]rotect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

Regulation S-ID (the "red flags rules"), adopted in 2013, requires covered entities to develop and implement a written, board-approved program that will identify and detect the warnings signs - "red flags" - of identity theft.

Applicable state privacy and data security laws must also be considered. For example, California's Online Privacy Protection Act (CalOPPA) requires operators of commercial websites or "online services" (such as smartphone "apps") to conspicuously post (or in certain cases make available) privacy policies if the site or service collects certain user information. Although the law applies only to the collection of information regarding consumers residing in California, it has a de facto nationwide reach. Earlier this year, California's legislature updated CalOPPA with new disclosure requirements related to certain tracking of consumer activities while using the site or service.

State data privacy laws can pose a real enforcement risk. Although state enforcement efforts may not focus on the financial services industry, they have targeted tools and technologies commonly used by many consumer-focused industries.

California Attorney General Kamala Harris, who was recently elected to a second term, has made data privacy and cybersecurity an enforcement priority. During her first term, Harris created a Privacy Enforcement and Protection Unit in the state's Department of Justice, which focuses on the civil prosecution of privacy laws. That same year Harris forged an agreement with several leading app platforms to ensure that users could find and review privacy policies before downloading a smartphone app. Many expect that Harris will continue to focus on data security and cybersecurity enforcement during her second term.

New, Enhanced Clarity at the Federal Level

Until the SEC's Risk Alert earlier this year, guidance on data privacy and cybersecurity had been broadly presented. The alert provided more granular, task-specific guidance by providing sample information requests that OCIE might use in examinations. These shed a much needed light on the depth of compliance readiness that the SEC expects.

The sample inquiries focus on a firm's ability to: self-identify cybersecurity risks; protect networks; ensure secure remote access and transfer requests; safeguard client information from third parties (including those who have been granted access, such as vendors and business partners); detect unauthorized activity; recover from an adverse cybersecurity event; appropriately monitor and respond to new cybersecurity regulations; and adapt to an evolving cybersecurity landscape.

Of course, the sample inquiries provide a non-exhaustive list of where an inquiry may focus. The set of inquiries actually posed to any particular firm likely will be tailored to that firm's risk profile. In addition to reviewing the Risk Alert, those seeking more information should review the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity," also published this year. SEC Commissioner Luis Aguilar said this framework may provide a "conceptual roadmap" for firms assessing possible cybersecurity measures.

OCIE Examination Preparation

In anticipation of further OCIE examinations, compliance professionals at all investment management firms, even those with data privacy and cybersecurity policies in place, should evaluate the completeness and effectiveness of those programs. Such an evaluation should at a minimum include the following steps.

First, assign responsibility and document relevant roles. Involve senior management, secure any necessary board approvals, and ensure awareness of these issues at all levels.

Know which laws apply to the firm, including state regulations. Read OCIE's Risk Alert, and analyze potential cybersecurity risks and vulnerabilities to understand how the firm would respond to each inquiry if examined. In addition, familiarize yourself with relevant industry standards.

Evaluate your own set of risks. Recognize that if your firm faces a risk, it's likely a risk for other firms, too. The more widespread the risk, the more likely it is to draw regulatory attention. In addition, learn whether internal policies are being followed, and confirm that the firm's practices are consistent with disclosure in the firm's client-facing privacy policies. Evaluate relationships with third parties and service providers, particularly if they receive or might gain access to customer information. Ensure appropriate contractual protections are in place.

Address the identified risks and disclosure obligations. Inventory the electronic means by which the firm communicates with its clients and the public, and confirm that the firm's privacy policies are posted in a manner that complies with applicable federal and state privacy laws.

Finally, plan the next periodic risk assessment. The risks in this area are always evolving, and the way firms address them should evolve accordingly.

Takeaways

There is no question that cybersecurity is on the radar of state and federal authorities. OCIE's Risk Alert provides an opportunity for firms to take stock of their current policies and practices and potentially discover new vulnerabilities. Firms should make a conscious and continuing effort to keep abreast of the quickly changing regulatory environment.


KEVIN F. CAHILL
Dechert


D. BRETT KOHLHOFER
Dechert

Kevin F. Cahill *is a partner in Dechert LLP's Orange Country office.* **D. Brett Kohlhofer** *is an associate in the firm's Washington, D.C. office.*