Featured Professionals

Sten-Erik Hoidal, CIPP

Related Services

Data Privacy & Security

Investment Management

Technology & Data

Emerging Trend: States Adopting Cybersecurity Regulations for Financial Services Industry

Legal Update
07.17.2017

New cybersecurity regulations impacting broker-dealers and investment advisers in Colorado went into effect over the weekend. The regulations from the Colorado Division of Securities (the Division) are intended to:

- "clarify what a broker-dealer and investment adviser must do in order to protect information stored electronically;" and
- provide "guidance to broker-dealers and investment advisers on what factors the Division will consider when determining if the procedures [employed] by the firm are reasonably designed to ensure cybersecurity."

By adopting these new regulations, Colorado confirms a trend toward state regulation and oversight of financial services entities' cybersecurity practices.

The cornerstone of the Colorado regulations is an obligation for broker-dealers and investment advisers to establish and maintain written procedures designed to "ensure cybersecurity" and protection of Confidential Personal Information (CPI).

CPI is defined broadly to include (1) social security numbers, (2) driver's license or other identification card numbers, (3) account, credit or debit card numbers, together with any required security code, access code or password that permits access to a Colorado resident's financial account, (4) digitized or electronic signatures, and (5) user names, unique identifiers, or email addresses in combination with passwords, access codes, security questions, or other authentication information that permit access to online accounts.

To the extent possible, a financial services firm's written cybersecurity procedures must include the following:

- An annual assessment by the firm or its agent of the potential risks and vulnerability to the confidentiality, integrity and availability of CPI;
- The use of secure email, including encryption and digital signatures, for communications containing CPI;
- Authentication practices for employee access to electronic communications, databases and media;

- Procedures for authenticating client instructions received via electronic communication (presumably to ward against phishing attacks, among other items); and
- Disclosure to clients of the risks of using electronic communications.

The Division, in turn, will review the reasonableness of broker-dealers and investment advisers' cybersecurity procedures. In doing so, the Division may consider a (1) firm's size, (2) relationships with third parties, (3) cybersecurity policies and practices and employee training, (4) authentication practices, (5) use of electronic communications, (6) auto-locking of devices with access to CPI, and (7) process for reporting lost or stolen devices.

The Colorado cybersecurity regulations are similar in objective to the New York Department of Financial Service's regulations that went into effect in March, although less overtly prescriptive. These regulations are another harbinger of changes to come on the state level, and a further warning to broker-dealers and investment advisers to formalize and harden their cybersecurity programs.