The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 31424

October 8, 2018

California Enacts First Law Requiring Manufacturers to Equip Internet-Connected Devices with Security

[31424]

October 8, 2018

TO: ICI Members
Investment Company Directors
Chief Information Security Officer Advisory Committee
Technology Committee SUBJECTS: Cybersecurity
Technology & Business Continuity RE: California Enacts First Law Requiring Manufacturers to Equip Internet-Connected Devices with Security

Governor Jerry Brown of California recently signed into a law two identical bills – one from the Assembly and one from the Senate[1] – that will require a manufacturer[2] of a "connected device"[3] to have "a reasonable security feature or features." Under the law, to be reasonable, the security feature must be:

- Appropriate to the nature and function of the device;
- Appropriate to the information it may collect, contain, or transmit; and
- Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

Also, if a "connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature if either: (1) the preprogrammed password is unique to each device manufactured; and (2) the device contains a security feature that requires a user to generate a new means of authentication[4] before access is granted to the device for the first time.

The law clarifies that it shall not be construed to:

- Require a manufacture to provide security for any unaffiliated third-party software or applications that a user adds to a connected device;
- Impose any duty "upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance" with the law;
- Impose upon the manufacturer of a connected device to prevent a user from having

full control over the device, including the ability to modify the software or firmware running on the device at the user's discretion;
- Apply to any connected devices whose functionality is subject to security requirements under federal law or federal regulatory authority;
- Provide a basis for a private right of action; and
- To limit the authority of a law enforcement agency to obtain connected device information from a manufacturer as authorized by law or pursuant to an order of a court of competent jurisdiction.

As noted above, the law provides no private right of action. Instead, it may only be enforced by California's Attorney General or by a city, county, or district attorney.

These bills were each signed into law on September 28th and become operative on January 1, 2020.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] The two bills are (1) California Assembly Bill 1906, which is available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB1906 and (2) Senate Bill 327, which is available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.

[2] As defined in Section 1798.91.05(c) of the law, the term "manufacturer" means "the person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California."

[3] "Connected device" is defined in Section 1798.91.05(b) to mean "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address."

[4] "Authentication" is defined in Section 1798.91.05(a) to mean "a method of verifying the authority of a user, process, or device to access resources in an information system."