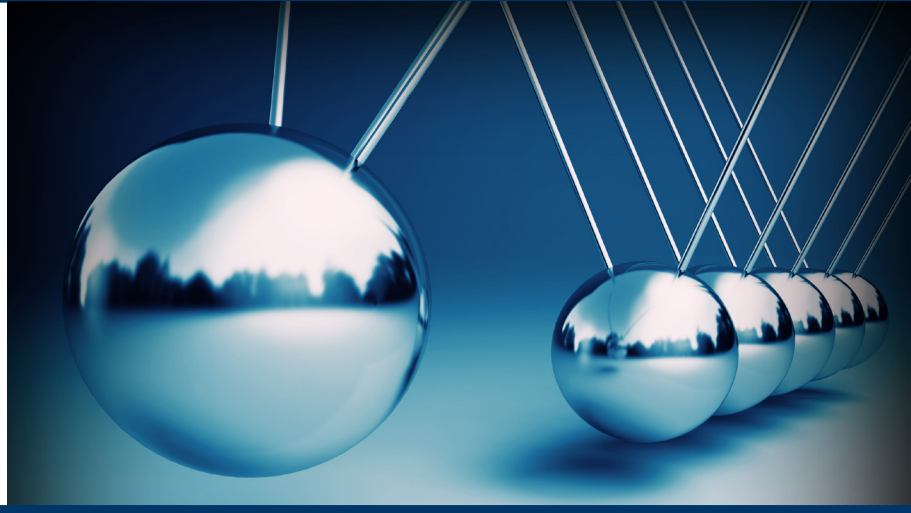
MURTHA MEANS MORE INFORMATION



INFORMATION SECURITY AND PRIVACY GROUP NEWS

March 2015

The Anthem data breach and the response of Connecticut's legislature

In the last few weeks, much has been written about the Anthem data security breach, which affected about 80 million Americans in 14 states. Anthem, the second largest health insurance company in the country, was holding personal information on current and former customers. The breach affected even some non-customers because Anthem also manages paperwork of several independent insurance companies.

Many of the impacted states reacted quickly and took measures to protect their constituents. Connecticut has been particularly active in this regard: just last week, the state's Attorney General, George Jepsen, announced the formation of a Data Security division within the Attorney General's office. This division will expand on the work of a privacy task force which has been in place since 2011.

Connecticut has truly been on the forefront of dealing with cybersecurity issues. Governor Malloy was recently appointed by the President to serve on a 10-member Council of Governors to lead discussions on cybersecurity. Congressman Jim Himes is a Ranking Member of Subcommittee on National Security Agency and Cybersecurity, and George Jepsen is a member of the National Association of Attorneys General Committee on Internet Safety/Cyber Privacy and Security.

In response to the Anthem breach, the Connecticut legislature jumped at the opportunity to protect the state's consumers against unauthorized use of their personally identifiable information. Not one, but two bills have been introduced to date during the current legislative session. Senators Looney and Duff, both Democrats, sponsored SB 1024, "An Act Concerning the Security of Consumer Data." The bill proposes that insurance companies, health care centers, entities licensed to do health insurance business in the state of Connecticut, pharmacy benefits managers, and third-party administrators who administer health benefits, would be obligated to implement encryption technology and would have to use it whenever transmitting "personal information." This is defined as a combination of an individual's first name or first initial and last name, in combination with a) a Social Security number, b) a driver's license or state identification number, c) an address, or d) identifiable health information. The bill also envisions that the Commissioner of Consumer Protection would adopt regulations to establish minimum standards for such encryption technology.

If you have any questions about the issues addressed here, or any other matters involving Information Security and Privacy issues, please feel free to contact:

Robert J. Munnelly, Jr., Chair
rmunnelly@murthalaw.com

Susan J. Baronoff
sbaronoff@murthalaw.com

Heather O. Berchem
hberchem@murthalaw.com

Stella Szantova Giordano
sgiordano@murthalaw.com

Rachel Snow Kindseth
rkindseth@murthalaw.com

James F. Radke
jradke@murthalaw.com

Stephanie Sprague Sobkowiak
ssobkowiak@murthalaw.com

Edward B. Whittemore
ewhittemore@murthalaw.com

This E-Blast is an overview intended to advise you of key aspects. If you have any questions or would like further information, please contact your attorney or a member of the Information Security and Privacy Group.

The second bill, Committee Bill No. 589 called "An Act Concerning the Unauthorized Access to Consumer Data," was introduced by Governor Malloy. The language of the bill is very similar to that of SB 1024, only in addition to the entities identified in the other bill, No. 589 would also apply to "banking or financial organizations." These terms are not defined, but the bill would likely apply to, at a minimum, all banks and credit unions. In addition, it could also extend to a wide variety of entities engaging in a "financial business," such as financial planners, accountants, tax advisers, investment advisers or broker-dealers.

On March 5, the Insurance and Real Estate Committee heard public testimony regarding SB 1024. While commentators applauded the efforts of the legislature to prevent future security breaches similar in magnitude to the Anthem breach, they raised concerns about passing a bill in isolation from more concerted national legislation that would set guidelines for what levels of cyber protection businesses were expected to maintain. Another concern is that since new technologies develop extremely quickly, requiring businesses to implement a certain level of encryption may cause more harm than good because the technology mandated by the law may be obsolete by the time the new law takes effect. Lastly, a trade group for the insurance industry expressed concern that asking businesses to adopt a specific security measure would only give hackers a roadmap for how to get around companies' security systems.

Commentators believe that SB 1024 will likely make it out of committee, but after that, it is an even chance as to whether the bill will be adopted. At present, expectations for the success of bill No. 589 are unknown. We will continue to monitor both pieces of legislation and will report on any new developments.

If you have any questions regarding the information included in this bulletin, please contact Edward B. Whittemore at ewhittemore@murthalaw.com / 860.240.6075, Stella Szantova Giordano at sgiordano@murthalaw.com / 860.240.6133, or any member of the Information Security practice group.