Recent Developments in Cybersecurity and Data Privacy

hugheshubbard.com client advisory

California Expands its Data Breach Notification Law

On Sept. 13, 2016, California Gov. Jerry Brown signed AB 2525, amending the state's data breach notification law. The existing law requires businesses to disclose breaches of unencrypted information. The amendment, which takes effect Jan. 1, 2017, expands the notification requirement to include encrypted information that is leaked with an encryption key or security credential that could render personal information "readable or useable."

The Yahoo Data Breach

On Sept. 22, 2016, Yahoo announced that it had suffered a massive data breach in late 2014 that compromised at least 500 million accounts. The compromised data included names, account passwords and other information but, according to the company, no payment card data. The very next day, three class actions were filed against Yahoo in federal courts in California and Illinois. A few days later, six U.S. senators wrote to CEO Marissa Mayer demanding to know what went wrong and how Yahoo intends to safeguard data in the future. Since then, Yahoo's troubles have continued to multiply as Verizon has asked for a $1 billion discount off its pending $4.8 billion acquisition.

Still More Calls for Federal Legislation

On Sept. 15, 2016, John Carlin, assistant attorney general for national security, called for a unified federal breach notification law, noting that it is "ridiculous -- and only a boon for lawyers -- that we have 47 different data breach notification laws."

On Sept. 27, 2016, five days after the Yahoo data breach was announced, the Federal Trade Commission (FTC) testified before a Senate committee. During its testimony the FTC again called for federal legislation that would "(1) strengthen its existing data security and (2) require companies, in appropriate circumstances, to provide notification to customers when there is a security breach."

Cybersecurity for the Presidential Election

On Oct. 6, 2016, Secretary of Homeland Security Jeh Johnson disclosed that 24 state election officials had approached the Department of Homeland Security for cybersecurity assistance in the run up to the Nov. 8 elections. The requests come weeks after it was reported that Russian hackers had attempted to breach voter registration databases in Illinois and Arizona.

Cybersecurity Makes the Debate

Our thanks to Lester Holt for raising cybersecurity at the first presidential debate. Both Democratic presidential nominee Hillary Clinton and Republican presidential nominee Donald Trump recognized cybersecurity as a pressing issue for the next administration and vowed to combat cyberattacks that threaten personal data and trade secrets.

In the Courts: Plaintiffs Need Economic Loss to Show Damages

The Seventh Circuit has been eroding the standing requirement to the point where plaintiffs can show standing without any economic loss. But plaintiffs still need to show economic loss to plead damages, which is an essential element of their claims. In the *In re Barnes & Noble Pin Pad* litigation, Judge Andrea Wood dismissed a consumer class action arising from the largest U.S. bookstore chain's 2012 data breach, finding that, while plaintiffs had pled standing under the prevailing Seventh Circuit precedent, they had failed to allege economic damages to support their claims.

Cybersecurity of Medical Devices

On Oct. 4, 2016, Animas warned of a potential cybersecurity risk with its OneTouch Ping insulin pump. The pump is not connected to the internet on any external network, but uses an unencrypted radio frequency communication system that could theoretically be hacked. The company noted that the risk of this happening is "extremely low" and would require "technical expertise, sophisticated equipment and proximity to the pump."

The United Kingdom Imposes a Record Fine

In the UK, the Information Commissioner's Office imposed a record-setting £ 400,000 fine on TalkTalk for its 2015 data breach. TalkTalk has been criticized because of the ease with which the hackers -- who are thought to be two teenage boys -- penetrated its security systems. Commissioner Elizabeth Denham explained, "hacking is wrong, but that it not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information." Denham further commented that the purpose of the record fine was to act "as a warning to others that cybersecurity is not an IT issue, it is a boardroom issue."

For more information, please contact:

Dennis Klein, *Partner*
+1 (305) 379-5574
dennis.klein@hugheshubbard.com

Seth Rothman, *Partner*
+1 (212) 837-6872
seth.rothman@hugheshubbard.com

Tyler Grove, *Associate*
+1 (202) 721-4625
tyler.grove@hugheshubbard.com

October 2016

Hughes Hubbard & Reed

Hughes Hubbard & Reed LLP
A New York Limited Liability Partnership | One Battery Park Plaza
New York, New York 10004-1482 | +1 212-837-6000