MINTZ

The February 2017 Update – The Mintz Matrix

February 16, 2017 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

As our readers know we maintain a summary of U.S. state data breach notification laws, which we refer to as the "Mintz Matrix." **Our latest update is available here, and it should be part of your incident response "toolbox" and part of your planning.**

During 2016, amendments to breach notification laws in five states went into effect (California, Nebraska, Oregon, Rhode Island and Tennessee). And by the end of last year, **well over twenty states had introduced or were considering new regulations or amendments to their existing security breach laws**. We expect there to continue to be significant regulatory activity in the data security space during 2017. As always, we will keep you abreast of changes and will release updated versions of our **Mintz Matrix** to keep pace with developments in the states.

We are keeping an eye out for signs of support for a national breach notification law. So far, there does not appear to be much political motivation for undertaking this effort. A key sticking point is anxiety among a number of states that a federal law would offer less protection than their existing state law. This is a valid concern since a national standard will only alleviate the significant burden of complying with the present patchwork of state laws if it has broad pre-emptive effect. Only time will tell if state and federal lawmakers can work together to develop a comprehensive nationwide regime for security breach notification and remediation.

In the meantime, we must keep tabs on the forty-seven states (along with the District of Columbia, Guam, Puerto Rico and the Virgin Islands) with their own security breach laws. Here is what's been happening since our previous update in the Fall:

California

California amended its security breach law in order to require disclosure to affected residents (and to the Attorney General if more than 500 Californians are affected) when encrypted personal data is acquired by an unauthorized person together with an encryption key or security credential that could render the personal data readable or useable.

We note also that former Congressman Xavier Becerra recently took over as Attorney General in California, replacing Kamala Harris who aggressively pursued regulation in the privacy arena during her tenure as AG and who now serves California as one of its U.S. Senators. Given this change in leadership, it will be interesting to see if the state continues to be a leader in pushing for stringent data security and privacy measures at the state and federal level.

Illinois

Last summer Illinois passed an amendment to its Personal Information Protection Act ("PIPA") that significantly broadened protections for personal information and the obligations imposed on businesses that handle such data. The amendment became effective on January 1, 2017 and made several key changes to PIPA:

- Definition of Personal Information. PIPA's definition of "personal information" has now been expanded to include medical information, health insurance information, and unique biometric data used for authentication purposes (examples cited in the statute are a fingerprint, retina or iris image, or unique physical representations or digital representations of biometric data). The amended definition also encompasses a user name or email address in combination with a password or security question and answer that would permit access to an online account when either the user name or email address, or password or security question and answer, are not encrypted or redacted.
- Encryption Safe Harbor. While PIPA already provided a safe harbor for data collectors if data disclosed due to a security breach was fully encrypted or redacted, the amendment clarified that the safe harbor does not apply if the keys to unencrypt or unredact or otherwise read compromised encrypted or redacted data have also been acquired in connection with the security breach.

- Nature of Notification. For security breaches involving a user name or email address in combination with a password or security question and answer, data collectors may now provide notice in electronic or other form to affected Illinois residents. Such notice must direct individuals to promptly change their user name or password and security question and answer, or to take other appropriate steps to protect all online accounts for which the affected resident uses the same user name or email address/password or security question and answer. The amended statute also provides an additional option for substitute notice when residents affected by a security breach are confined to one geographic area.

- New Exemptions. The amendment added an exemption for data collectors who meet their obligations under applicable provisions of the Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"). Any data collector that provides notice of a security breach to the Secretary of Health and Human Services pursuant to its obligations under HITECH must also provide this notification to the Illinois Attorney General within five business days of notifying the Secretary. This exemption will primarily apply to certain entities operating in the healthcare space. The amended statute also deems financial institutions subject to applicable provisions of the Gramm-Leach-Bliley Act in compliance with PIPA's data security requirements.

- Security Requirements. Beyond addressing breach notification, the amendment requires covered entities to implement and maintain reasonable security measures to protect records containing personal information of Illinois residents and to impose similar requirements on recipient parties when disclosing such personal information pursuant to a contract. The amended statute also requires state agencies to report security breaches affecting more than 250 Illinois residents to the Illinois Attorney General.

Massachusetts

For those information junkies out there! The Office of Consumer Affairs and Business Regulation (the "OCABR") in Massachusetts has created a public web-based archive of data breaches reported to the OCABR and the Massachusetts Attorney General since 2007. The data breach notification archive is available at **www.mass.gov/ocabr** and includes information about which entity was breached, how many Massachusetts residents were affected, if the breach was electronic or involved paper, and the nature of remediation services offered to affected residents.

It is always a good time to review your incident response plan and data privacy policies to bring everything in line with changes happening on the state level.

And now for the disclaimer: The **Mintz Matrix** is for informational purposes only and does not constitute legal advice or opinions regarding any specific facts relating to specific data breach incidents. You should seek the advice of the Mintz Levin privacy team or other experienced legal counsel when reviewing options and obligations in responding to a particular data security breach.

Make sure to get your February 2017 Mintz Matrix! **Available here** for downloading and always linked through the blog's right-hand navigation bar.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.