MINTZ

Illinois Joins the Fray: Strengthens its Laws Around Data Breach Notification and Data Security

June 14, 2016| Blog | By Michael Katz, Julia Siripurapu, **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

Sophisticated phishing scams and muscular hacking efforts continue to compromise personal and sensitive information held by insurers, hospital systems, and businesses large and small. In response, many states have strengthened their data breach notification and have enacted data security laws to enhance data protection obligations imposed on data collectors and to ensure that residents and state regulators receive prompt and adequate notice of security breaches when they do occur. By mid-summer, a range of new measures will be going into effect in Nebraska, Nevada, Rhode Island and Tennessee. Be sure to review the latest edition of the **Mintz Matrix** for these new measures.

And now Illinois has become the latest state to take action by recently passing amendments to its Personal Information Protection Act ("PIPA"). Effective as of January 1, 2017, the changes will principally (i) broaden the statute's definition of "personal information," (ii) clarify the encryption safe harbor, (iii) address the form and content of certain required notification to residents, and (iv) establish limited exemptions from PIPA. Illinois has posted the text of its **amended statute** and we will provide further detail on each aspect of the coming changes. Here is a summary of the key changes to PIPA:

1. *Definition of Personal Information*. PIPA's existing definition of "personal information" captures an individual's first name or first initial and last name in combination with any one or more of the following data elements: Social Security number, driver's license number or state identification card number, or account number or credit or debit card number with or without any required security code, access code or password permitting access to the individual's financial account. The definition requires either the name or a data element to be unredacted or unencrypted. When the amendments become effective, the definition will be 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 will also encompass 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.
2. *Encryption Safe Harbor.* Both the existing and amended versions of PIPA provide a safe harbor for data collectors if data disclosed due to a security breach is fully encrypted or redacted. However, the amendments to PIPA clarify that the safe harbor will 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.
3. *Nature of Notification.* For security breaches involving a user name or email address in combination with a password or security question and answer, the PIPA amendments will permit data collectors to provide notice in electronic or other form to affected Illinois residents directing such individuals to promptly change their user name or password and security question or 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 and password or security question and answer. The PIPA amendments also provide an additional option for substitute notice when residents affected by a security breach are confined to one geographic area.
4. *New Exemptions.* Although Illinois will expand the range of personal information subject to its data breach notification law, the PIPA amendments will simultaneously add 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 will also need to 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 PIPA amendments will also deem financial institutions subject to applicable provisions of the Gramm-Leach-Bliley Act in compliance with PIPA’s data security requirements.

5. *Security Requirements.* Beyond addressing breach notification, the PIPA amendments will require 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 PIPA amendments will also require state agencies to report security breaches affecting more than 250 Illinois residents to the Illinois Attorney General.

Unfortunately, security breaches involving personal information are becoming all too commonplace and for that reason alone we do not expect the pace of regulatory developments in the data security arena to slow down. You should seek the advice of experienced legal counsel (e.g., **the Mintz Levin privacy team**) when reviewing options and obligations in responding to a particular data security breach.

Authors

Cynthia J. Larose, Member / 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.