PRIVACY AND DATA SECURITY ALERT

JUNE 6, 2016

SHOOK
HARDY & BACON

ILLINOIS MAKES WIDE-RANGING CHANGES TO ITS IPIPA

Illinois recently amended its Personal Information Protection Act (IPIPA), and the changes take effect January 1, 2017. The amendments make significant changes to the IPIPA that affect any entity that deals with nonpublic personal information. In particular, the new IPIPA includes new disclosure requirements for wide categories of information, and failure to comply with the IPIPA could potentially lead to penalties for unwary businesses. Key changes to the IPIPA include the following:

- **Broader Definition of Personally Identifiable Information.** The amended IPIPA broadens its definition of personally identifiable information (PII), adding four new categories of PII to already established ones such as Social Security numbers and account numbers. For three of these new categories to qualify as PII, they must be disclosed in conjunction with an individual's first name or initial and last name. These are: (1) health insurance information, (2) medical information and (3) biometric data. The fourth category is new to Illinois: an individual's online username and password or security question combinations, if these combinations are disclosed in a manner that would permit access to an online account. These changes are spurred by the realization that consumers are increasingly submitting and storing personal information online, including health information, and, unfortunately, often using the same usernames, passwords and security questions. This expanded definition will likely result in an increased number of data breaches under the law.

- **New Provision Regarding Notification of Breach of Username Information.** In the event of a breach involving username and password/security question combinations, the amended IPIPA directs the data collector to provide notice to anyone whose data has been compromised and advise them to promptly change his or her username, password and/or security question(s). Notification procedures for breaches involving other types of PII remain largely unchanged.

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Matthew Wolfe
dd 312.704.7777
mwolfe@shb.com

Al Saikali
dd 305.960.6923
asaikali@shb.com

- **Security Requirements for Illinois Data Collectors.** The new IPIPA also implements new requirements for data collectors storing PII of Illinois residents. It requires that data collectors maintain "reasonable security measures" to protect those records from unauthorized access. It also requires all contracts for the disclosure of Illinois residents' PII maintained by a data collector (for example, contracts with vendors of the data collector) to include a provision requiring the recipient of that information to implement reasonable security measures to protect the PII.
  Importantly, the IPIPA provides no guidance as to what is meant by "reasonable security measures." However, as noted in a recent report by California's attorney general, federal and state agencies around the country have offered guidance on what constitutes reasonable data security. Generally, this requires a risk management approach focused on continuous identification and assessment of risks, implementation of controls and monitoring of those controls' effectiveness.

- **Safe Harbor for Compliance with Federal Law.** Finally, the amended IPIPA creates several safe harbors for companies that are in compliance with other federal laws. First, it expressly states that a data collector subject to and in compliance with the standards set out by the federal Gramm-Leach-Bliley Act (which generally applies to financial institutions) is also in compliance with IPIPA. Second, it provides that an entity subject to and in compliance with the federal Health Insurance Portability and Accountability Act's privacy and security standards is also in compliance with the IPIPA, so long as the entity meets its reporting obligations under both Acts. Third, it generally states that if a data collector is in compliance with any state or federal law setting higher standards than the IPIPA, it also is in compliance with the IPIPA.

In short, the recent changes to the IPIPA are consumer-friendly changes that will increase the number of data incidents that are considered breaches and therefore require notification. The changes also will require the implementation of new requirements on businesses that store Illinois residents' PII.