FOLEY & LARDNER LLP

Summary of Amendments to State Data Breach Notification Laws in 2016

NOTE: This chart only includes amendments for those states that enacted changes in 2016, effective in either 2016 or 2017. Those states that enacted amendments in 2015, and which became effective in 2016, are not covered by this chart. This chart is for informational purposes only and does not constitute legal advice or opinions.

	Definition of "Personal Information"	Notification	Encryption Safe Harbor	Carveouts for Compliance with Other Privacy Laws
 Trend	Expanded definition of "personal information"	Redefined timing and content of notification and added requirement that notice go to the state attorney general	Removal of safe harbor for data that is encrypted, unreadable, unusable, or redacted, if the confidential process or key was also acquired	Carveout provided to entities subject to and in compliance with Gramm-Leach-Bliley Act (GLBA) or Health Insurance Portability and Accountability Act (HIPAA)
 Arizona				Amended to provide an exemption to business associates of covered entities as defined under HIPAA.
 California			Notification required if (1) "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the agency that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable."	

FOLEY

FOLEY & LARDNER LLP

	Definition of "Personal Information"	Notification	Encryption Safe Harbor	Carveouts for Compliance with Other Privacy Laws
 Illinois	Expanded the categories of "personal information" to also include: health insurance information; "medical information"; "unique biometric data"; and an individual's user name or email address, in combination with a password or security question and answer that would permit access to an online account.	Requires notice to the Illinois attorney general of any data breach that impacts more than 250 Illinois residents, which must be provided within the sooner of 45 days of the discovery of the breach or when notification of the breach is sent to Illinois residents. For breaches of security involving individual user names or email addresses, the notice must direct the individual "to promptly change his or her user name or password and security question or answer, as applicable, or to take other steps appropriate to protect all online accounts for which the resident uses the same user name or email address and password or security question and answer."		Entities "subject to and in compliance with" Section 501(b) of the Gramm-Leach-Bliley Act (GLBA) will be deemed compliant. Entities subject to and adhering to conditions under the Health Insurance Portability and Accountability Act (HIPAA) will also be considered in compliance, except that if, under HIPAA, the entity is required to notify the U.S. Department of Health and Human Services of a breach, it must also notify the Illinois attorney general within five business days.
 Nebraska	Included "user name or email address, in combination with a password or security question and answer" in the definition of "personal information."	Added obligation requiring notice to the Nebraska attorney general whenever notice is given to a Nebraska resident.	Removed safe harbor for encrypted data if the "confidential process or key was or is reasonably believed to have been acquired" as a result of the breach of the security system.	
 Tennessee		Notification must be made to individuals no later than 45 days from the discovery of the breach or notification by a service provider that it has discovered a breach (which may be tolled to enable law enforcement to complete a criminal investigation).	Redefined "breach of the security system" to mean unauthorized acquisition of computerized data, deleting the qualification that the computerized data must be "unencrypted." However, definition of "personal information" is limited to data that is unencrypted.	Exempts entities and persons subject to HIPAA and GLBA.