THE
NATIONAL LAW REVIEW

Big Data Breaches Shine Spotlight on Laws Impacting Employee Data Protection

Monday, May 14, 2018

It seems like almost every week we learn of a massive new data breach, risking the loss of thousands of individuals' personal and confidential information to a faceless hacker halfway around the world.

A quick internet search for the latest news about data breaches reveals the sheer volume of information hacked or leaked on a daily basis, ranging from our Social Security and bank account numbers to protected health information, our consumer preferences, and more. And, of course, where there are breaches, there is litigation. In fact, just this week, the Seventh Circuit Court of Appeals (covering Illinois, Indiana and Wisconsin) ruled in favor of the plaintiffs in a consumer class action case where the alleged hack resulted in disclosure of customer names, credit and debit card numbers, expiration dates, and PINs.

Article By Foley & Lardner LLP
John L Litchfield
Labor and Employment Law Perspectives

Communications, Media & Internet
Labor & Employment
All Federal

But it's not just consumer data that's at risk – employers, too, collect and maintain the same kind of sensitive information and data about their employees as is often the subject of a data breach. A loss of control over that employee data can have a significant adverse impact on an employer's credibility and bottom line.

State legislators are taking note of the risks and a patchwork of new data privacy laws are popping up around the country. We've written before about some existing laws impacting how employers collect and maintain employee biometric data, such as fingerprints and facial or retinal scans. However, the scope of information subject to the new laws' protections is expanding, as are the notification requirements and penalties for failure to comply. To ensure compliance and protection of employee and consumer data alike, employers should therefore take note of the following state laws coming online in 2018:

- Alabama (effective June 1, 2018): The state's Data Breach Notification Act applies to any person or entity that uses sensitive personally identifiable information about Alabama residents, including non-truncated Social Security, driver's license, passport, military ID or other unique ID numbers issued on government documents, financial account numbers, medical history information, health insurance information, personal usernames and passwords, etc. The law also requires notification to an individual whose protected data is hacked.

- Delaware (effective April 14, 2018): Delaware's data breach law applies to all entities that transact business in the state. The legislation amended existing law to expand the definition of covered personal information to include biometric (e.g., fingerprints, retinal scans, etc.) and other health information, and imposed a 60-day notification deadline following a data breach

- Oregon (effective June 2, 2018): The Oregon data breach law, which applies to entities collecting personal information about any Oregon resident, was amended to include biometric and health information as data protected by the law, and requires that a breach be disclosed to the affected individual(s) within 45 days of discovery.

- South Dakota (effective July 1, 2018): South Dakota's data breach law applies to any person or entity conducting business in South Dakota that "owns or licenses" computerized personal or protected information of South Dakota residents. The law protects a broad swath of information, including

> "identification numbers assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data." Notice of a breach of any such data is required within 60 days of the breach, with fines of up to $10,000 per day per violation for failure to comply.

Additionally, for employers doing business in Canada, new laws impose a $100,000 per person per day penalty on any covered entity, including banks, telecommunications and broadcasting companies, and trucking companies, for failure to meet the federal notice of breach requirements.

And, of course, the much discussed European Union General Data Protection Regulation (GDPR), applicable to companies that monitor or process the personal data of European citizens, has strict requirements as to how such personal data is collected, stored and maintained.

In short, because nearly all employers collect and maintain at least some information subject to protection under the growing number of data protection laws around the world, it is important to understand what data is protected, any obligations imposed on employers regarding data that is collected, and, in the event of a breach, how and when to notify the affected individuals.

Source URL: https://www.natlawreview.com/article/big-data-breaches-shine-spotlight-laws-impacting-employee-data-protection