Lessons From Equifax - Trends on Data Breach of Employee Information

Matthew C. Luzadder

October 16, 2017

The recent Equifax breach data and public missteps in handling the breach has companies revisiting their cybersecurity measures and refreshing their breach response plans. Although not every company has consumer data likely to be targeted by hackers, employment files may be compromised, such as when breaches of U.S. government databases exposed the personally identifiable information (PII) of 22.1 million people, including not only federal employees and contractors but their families and friends. Breach incidents have a panoply of repercussions for businesses that suffer them, including reputational damage, loss of business, and legal repercussions. All states except Alabama and South Dakota require notification when information commonly maintained by employers, such as Social Security numbers and driver's license numbers, is compromised.

Liability for breaches will vary by state law. In 2017, two Pennsylvania courts shined some light on this issue. In both cases, which involved large-scale data breaches affecting thousands of employees, the courts absolved the employers of any potential liability because either (1) they owed no duty in tort to their employees to protect PII against data breaches or (2) the employer had no express or implied contractual obligation to protect the PII. *See Enslin v. Coca-Cola Co.* (E.D. Pa. Mar. 31, 2017); *Dittman v. UPMC* (Pa. Sup. Ct. Jan. 12, 2017), reargument denied Mar. 20, 2017. It's important to remember these laws are in their infancy and results will vary by state.

In 2016, Illinois expanded its employer data breach notification with the passage of the Personal Information Protection Act (effective January 1, 2017). *See* 815 ILCS 530/10(a)(2). The updates include the following:

- Illinois eliminated the ability to avoid notification because the compromised personal information was encrypted or redacted. Under the amended law, if encrypted or redacted personal information is breached, notification is still required if information needed to unencrypt or unredact the personal information is acquired with the encrypted personal information.
- "Personal information" was expanded to include, among other things, an individual's SSN, driver's license number, health insurance information, unique biometric data ("fingerprint, retina, or iris image, or other unique physical representation or digital representation of biometric data"), and an individual's user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account (i.e. log-in credentials). Now, obtaining any of this information triggers reporting requirements.
- Illinois employers are required to notice the Illinois Attorney General of any data breach that affects more than 250 Illinois residents. This notice must be provided within the sooner of 45

day of the discovery of the breach, or when the notification of breach is sent to Illinois residents.

As demonstrated by Illinois's recent amendments, data breach notification laws continue to evolve and expand in their attempt to adapt to heightened risks associated with increasingly sophisticated hacks and scams to gather personal information. While this post focuses on Illinois, employers should monitor the laws in the states where their employees reside for new developments.

In addition to monitoring the laws, employers should consider implementing the following:

- Take cybersecurity seriously and take steps to minimize the risk of data breaches, including exercising reasonable care in the management of personally identifiable information about employees;
- Review policies and codes of conduct related to the handling of data to ensure they are compliant with legislative changes (reach out to privacy or employment counsel for assistance monitoring legislative changes);
- Respond swiftly to suspected data breaches and other events – like the theft of computers – that could result in data breaches;
- When breaches occur, or are suspected, consider affirmative steps, such as paying for credit monitoring or identity theft protection, to address employees' fears; and
- Consider designating a security incident response team that conducts drills and/or simulations to test the effectiveness of the incident response plan.