Labor & Employment Group

## Responding to a Data Breach

*By Sarah E. Smith, Associate Attorney*

Your server has been hacked or you are the victim of a phishing scam, in which sensitive employee information has been exposed. You know you have a problem, but what do you do about it?

Start by reporting the data breach to the FBI, Federation of Tax Administrators, and the IRS. Local law may also require you to contact other entities, such as local law enforcement or state attorneys general.

Next, you need to notify the affected employees. While there are many privacy-related laws that regulate particular categories of information, such as HIPAA, there is no single comprehensive federal law regulating data breach. Bills have been introduced in Congress repeatedly over the years (as late as November of 2017), but all have failed to pass.

Instead, situations like this are governed by a patchwork of different state laws. Each of the states except Alabama and South Dakota has its own data breach notification laws, making things more complicated where a breach impacts employees residing in multiple states. The laws have different requirements as to when notice is required, what form of notice, whether other entities need to be notified, etc. Notice should be given even with a minor breach, given the potential for sensitive information to be exposed.

The notification letter that goes out to employees will therefore need to be tailored depending on which state it is sent to and that state's laws. Most state breach notification laws do not set out specific requirements for the notice's content. However, the notice generally should be in plain English and include the date of the notice, a brief description of the data breach incident in general terms, the date of the breach, the categories of personal information at issue, a brief description of the actions taken by the business to contain the breach and protect data from further unauthorized access or use, and contact information for law enforcement and national consumer reporting agencies. Additionally, some states impose timing requirements for providing the notice.

Finally, you may also consider taking additional steps to assist the impacted employees, including offering credit monitoring for one year free of charge, paying to freeze credit reports, providing identity theft insurance, and offering products that provide assistance to those employees experiencing fraud on their accounts, such as identity restoration services.

Should you experience a data breach, or for more information about state data breach notification laws, please contact a BPJ attorney.

Sarah E. Smith is a part of the Labor and Employment law group at Burch, Porter & Johnson. Additionally, her practice includes business and commercial litigation. Prior to joining Burch, Porter & Johnson, Ms. Smith served as a law clerk to the Honorable Bernice B. Donald of the United States Court of Appeals for the Sixth Circuit and the Honorable Sheryl H. Lipman of the United States District Court for the Western District of Tennessee.

If you have questions, please contact ssmith@bpjlaw.com.