Arnall Golden Gregory LLP

Client Alert

Contact Attorney Regarding This Matter:

Robert R. Belair
202.677.4040 - direct
202.677.4041 - fax
robert.belair@agg.com

WHAT YOU NEED TO KNOW TO AVOID AND RESPOND TO A DATA BREACH

Is My Company at Risk?

Large scale data breaches perpetrated by clandestine hacker organizations have made headlines and will continue to do so in the foreseeable future, but the headlines fail to adequately describe the breadth of the risks faced by companies across the United States. Your company may not be the target of the next big cyber-attack, but it may still face a very real risk of an expensive and damaging data breach.

Does My Company Maintain Sensitive Personal Information?

Certain industries immediately come to mind when considering the risks of a data breach—healthcare companies, financial institutions and educational institutions, such as colleges and universities. By their nature, these industries maintain a significant amount of data in which the average person would expect a certain level of privacy. Certainly, companies in these industries are on the leading-edge of risk and need experienced counsel to advise them—both before and after a breach—of the constantly-changing regulatory requirements.

But privacy regulations are not aimed solely at those industries and apply broadly to any business that maintains certain types of sensitive personal information including:

- Addresses and telephone numbers;
- Email addresses;
- Passwords;
- Credit card information;
- Bank account information; and
- Social security numbers.

Many companies store this type of information, both for marketing purposes and to facilitate future transactions. Moreover, companies frequently maintain this type of information on their employees, especially in light of recent regulations requiring the verification of citizenship.

Arnall Golden Gregory LLP
Attorneys at Law

171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031
404.873.8500

2001 Pennsylvania Avenue NW
Suite 250
Washington DC 20006
202.677.4030

www.agg.com

What are the Sources of a Data Breach?

The term data-breach brings to mind an anonymous computer hacker gaining access to a company's servers, but this picture does not tell the whole story. Certainly, some of the known data breaches involved the compromise of a computer system by some external person. The quantity of email viruses and scams attest to the prevalence of such activity. Almost an equal number of data breaches, however, involve an employee or former employee of the business. The threat of a data breach is not only "out there," but is as close as a disgruntled, opportunistic or careless employee.

Moreover, data breaches are frequently low-tech. A data breach can be as simple as the loss of a laptop computer or unencrypted discs, neglecting to properly shred sensitive documents, or the mis-delivery of information. These breaches trigger the same obligations and requirements as a malicious breach.

The threat of a breach is multiplied if your business shares any of the sensitive personal data with third-party vendors. Even if your company is entirely faultless, a disclosure by one of your business partners can lead to damaging consequences if not properly handled.

Has My Company Already Suffered a Breach?

Unlike the notorious "LulzSec" hacker organization, most individuals who steal confidential information do not post their theft on the internet. Accordingly, your company may have experienced, and continue to experience, a data breach without your knowledge. The detection of an inadvertent breach is oftentimes even more difficult to discover.

In this context, what you don't know, can hurt your company. If the breach leads to some harm to your customers or employees, it will likely be traced back to your company. Your company's failure to detect and mitigate the damages resulting from the breach will be used by those harmed to increase your company's liability. Moreover, prompt detection can, in many cases, allow you to prevent or lessen the harm caused by the breach and prevent the compromise of additional information.

What Can My Company Do to Protect Itself?

Some data breaches are inevitable, but a proactive approach to data security and prompt response to any known breaches go a long way to insulating your company from liability and minimizing the liability that remains. The lawyers in Arnall Golden Gregory LLP's Privacy Team and Data Breach Response Team can assist your company in complying with the myriad of federal and state regulations regarding the protection of sensitive personal data; in creating a proactive a data breach response plan; and in responding to a data breach if one ever occurs.