Arnall
Golden
Gregory LLP

The Washington Report by Montserrat Miller
Partner, Arnall Golden Gregory, LLP

Recently I came across an article regarding multiple data breaches and the executive of one company was actually receiving positive press relative to a data breach where individuals' personally identifiable information (PII) was compromised. Who knew such positive media coverage was possible! However, it wasn't the breach that was being lauded, but rather the company's response to the breach. Mind you that this could cut either way. Take the Sony Corp. example, where they were criticized for their consumer response when their PlayStation gaming system was hacked.

Given the sophistication of hackers, if you collect, use, maintain or disseminate PII you have a problem in that a data breach is one key stroke or one lost laptop away. It is important therefore to plan in advance, and have a written data security and breach notification policy in place, regarding if, who, how and when you will respond in the event of such a breach. Have a crisis response team in place, both internally and externally, which includes legal counsel, IT specialists and public relations experts. Recognize that consumer's PII is uniquely precious and the Holy Grail for identity thieves. While perhaps some hackers hack for the thrill of the challenge (super geeky) or others hack for military and espionage purposes (super bad), the type of hacker that you and I have to worry about on a daily basis is the one who steals credit card information or social security numbers for the purpose of committing identity theft.

Several important decisions need to be made upon discovery of a PII data breach, including whether to disclose, who to disclose to, how to disclose and when to disclose. Certain states require notice be sent immediately to in-state residents, such as Florida. Other states require that state officials be notified in addition to the affected consumers, such as Maine and Virginia. And finally, some states require certain language be included in the breach notice letter sent to in-state residents. Ahh, if only there was one Federal law....

While each state's nuanced approach to breach notification keeps me and my firm colleagues busy, it is challenging to navigate a company's response. Which brings me back to how and why I started this article -- have a data security and breach notification plan in place. Of course, it goes without saying to have in place strong safeguards, policies and procedures to protect PII in the first place. However, even the best laid plans can run afoul of our expectations. In a nutshell, all entities that deal in PII, especially PII such as names, credit card information or certain financial information, and social security numbers should ensure that they have a written policy in place to: (1) protect PII and prevent a breach through physical and technological barriers; (2) in the event of a breach, have a breach response plan spelled out to plug the leak and also prepare to systematically provide notice to affected consumers where notice is

triggered based on the PII that was compromised; and (3) provide notice to the appropriate consumers and state officials, in a timely and appropriate manner and with the necessary content per state law. In certain circumstances, given the size of the breach, you may also have to provide notice to the credit reporting agencies. These three points do not cover the full spectrum of steps to be taken, but I only have a maximum of 750 words in which to lay all of this out and the first question you should ask yourself – does your company have in place a data security and breach notification written policy? If not, contact me.