PULLMAN &COMLEY LLC
ATTORNEYS

Cyber Law TRACKER
Developments in Cybersecurity

A publication of Pullman & Comley, LLC

March 2012

Why Prevention May Be Much Less Costly Than a Cure - If There Even Is a Cure - When Dealing With Privacy and Security Matters

by *Steven J. Bonafonte* . Posted on March 21, 2012

We routinely hear stories about "data breaches," "identity theft," "credit monitoring," and other data loss-related events in the media. These reports are becoming more frequent – almost routine – and may run the risk of being overlooked by many companies – even those who are in the business of collecting, processing or otherwise using confidential information of individuals.

One recent case, however, illustrates why we should not fall victim to thinking that data breaches are "routine."

The Wall Street Journal recently reported on the bankruptcy of a national medical records firm after over 14,000 medical records were compromised during a burglary of their California offices in December 2011. The burglary occurred on 12/31/2011, and was discovered on 1/3/2012 and promptly reported to law enforcement. Nonetheless, the company was required to report the incident to various state and federal regulators as well as notify each of the potentially affected individuals.

In its explanation of why it was seeking relief under Chapter 7 bankruptcy the company stated that "The cost of dealing with the breach was prohibitive." Chapter 7 bankruptcy (unlike Chapter 11) is used when the company is to be liquidated and its proceeds distributed to its creditors, so it appears as if this firm is headed out of business permanently.

Fortunately, events such as this are usually avoidable with the right combination of preventive legal and technical counseling. It also is critical from a risk management and a business continuity perspective that companies have a legally defensible system of controls in place to meet their regulatory and contractual responsibilities. Having the minimum of: policies and procedures for managing sensitive personal data, technology controls such as encryption and other data loss prevention software, physical security and a critical incident response plan will go a long way toward avoiding this unfortunate result.

Continued

Subscribers to *The Wall Street Journal* can access the full article here.