No Business is Immune from Data Breach Says Scott & Scott, LLP

The recent publicly disclosed breach of a box-office and online ticketing service's data base highlights the fact that every business collecting, using, maintaining, or storing electronic data is at risk for a security incident. Scott & Scott, LLP, suggests companies have a data breach plan in place to prepare for and mitigate the liability, costs, and brand-damage associated with data security breaches or incidents

Southlake, Texas (PRWEB) June 27, 2013 -- Vendini, a California-based company that provides box-office and online ticketing services to hundreds of tour, casino, sports, arts, and entertainment venues and promoters across the U.S. and Canada, posted on its website on May 21, that they detected on April 25 that their web server was breached. According to a June 12th Lehigh Valley's The Morning Call article, a company spokesman said they are sending letters in waves to those who may have been impacted.

The company has not disclosed how many people may have been affected. A May 23rd article in SC Magazine says the hack possibly affected at least tens of thousands of people.

Vendini is not alone. They have lots of company. It's unusual not to read a daily headline reporting a data breach either in retail, financial, healthcare, social networks, social media, and government agencies.

"Every business collecting, using, maintaining, or storing electronic data is at risk for a security incident. Even those companies who have implemented the most advanced security initiatives are not immune from data breaches", said Robert J. Scott, Managing Partner, of Scott & Scott, LLP, with a practice area focus on privacy and security.

Scott & Scott, LLP recommends companies:

(a) implement preventive measures to minimize the threat of a notice-triggering event including privacy policies and procedures, ongoing privacy training, and proactive technology measures such as data encryption
(b) hire expert counsel or forensics services to investigate the incident
(c) know appropriate breach notification requirements and what immediate remedial action to implement in accordance with the law
(d) minimize the legal liabilities, damage to reputation, and costs associated with data breach by taking appropriate action within statutorily required timeframes.
(e) avoid over or under-reporting the incident.

"After a security incident occurs, time is of the essence", continued Scott.

A downloadable copy of Scott & Scott, LLP's state data breach chart is available at: http://www.scottandscottllp.com/main/uploadedFiles/resources/Publications/state_data_breach_notification_law.pdf

About Scott & Scott, LLP
Scott & Scott, LLP is an intellectual property and technology law firm dedicated to helping senior executives assess and reduce the legal, financial, and regulatory risks associated with information technology issues. An innovative approach to legal services, Scott & Scott, LLP believes that collaboration between legal and

technology professionals is necessary to solve and defend against the complex problems our clients face, including privacy and network security, IT asset management, software license compliance, and IT transactions. Legal and technology professionals work in tandem to provide full-service representation. By combining these resources, Scott & Scott, LLP is better able to serve clients' needs than law firms and technology services firms working independently of one another.

Visit Scott & Scott, LLP online at www.scottandscottllp.com
-30-

Contact Information
Anita Scott
Scott and Scott, LLP
http://www.scottandscottllp.com
214.999.2915

Online Web 2.0 Version
You can read the online version of this press release here.