DuetsBlog
COLLABORATIONS IN CREATIVITY & THE LAW
www.DuetsBlog.com

*A Winthrop & Weinstine blog dedicated to bridging the gap between legal & marketing types.*

# Data Security in the Cloud

Posted on April 29, 2011 by Brad Walz

It didn't take long for the lawsuits to start after Sony notified 77 million PlayStation Network and Qriocity online service customers that their credit-card data, billing addresses, and other personal information might have been stolen. On April 27th, Johns v. Sony Computer Entertainment America LLC was filed in the United States District Court for the Northern District of California in San Francisco. Kristopher Johns, the lead plaintiff in the class action suit, said in the Complaint that "Consumers and merchants have been exposed to what is one of the largest compromise of Internet security and the greatest potential for credit-card fraud to ever occur in United States history."

Because the use of cloud computing services is becoming more prolific, as a business that may store customer data in the cloud, it is support to understand what legal responsibilities exist in the event of a data security breach. Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. Only Alabama, Kentucky, New Mexico, and South Dakota do not have security breach laws. Generally, the time for making the required notification is not set in stone, but must be made in the most expedient time possible and without unreasonable delay. If you are storing personal identifiable information of your customers in the cloud, make sure you are familiar with the data security breach notification laws.

But today is not the day to be talking about negative things. After all, it is the royal wedding of Prince William and Kate Middleton. So congratulations to the newly weds!