Using Vendor Agreements to Protect Against Data Breaches

By Julie Machal-Fulks

The recent Target data breach, one of the largest breaches in history, appears to have been initiated after intruders used stolen vendor credentials to access Target's point-of-sale system and install malware. Even if Target had no issues with its internal security, the trust it placed on one of its vendors has already yielded federal criminal investigations, and will likely result in millions of dollars of remedial measures to protect customers' identities after the data breach.

When outsourcing data, companies that use personally identifiable information must ensure that every vendor, reseller, or service provider who has access to the information has sufficient protections in place to reduce the risk of a security incident. Many security incidents result from lack of physical security rather than lack of technological security. For instance, misplaced laptops, unlocked data centers, and post-it notes containing login credentials all result in many security breaches every year.

Companies that outsource any part of their data management have to ensure that their agreements with their business associates contain assurances that not only the technological security is sufficient but also that the physical measures to protect the data will be appropriate given the potential security risks. Agreements must also require the business associates to obtain and maintain appropriate insurance to cover any security incidents and to agree that the entity responsible for the breach will be responsible for the defense costs associated with any investigation or lawsuit.

Any company that maintains personally identifiable information should work with experienced counsel to ensure that its agreements contain appropriate protections.

About the author Julie Machal-Fulks:

As a partner at Scott & Scott, LLP, Julie Machal-Fulks leads a team of attorneys in representing and defending clients in legal matters relating to information technology. Her practice focuses on complex litigation ranging from privacy and network security, data breach notification and crisis management, intellectual property disputes, service provider negligence claims, and content-based injuries such as copyright and trademark infringement in software, the Internet, and all forms of tangible media.

Get in touch: jfulks@scottandscottllp.com | 800.596.6176