HARTMAN LAW PLC

Could You be Sued if Your Customer Database is Breached?

Hartman Law PLC
7114 E. Stetson Drive
Suite 205
Scottsdale, AZ 85251-3250

T: 480.659.0019
F: 480.659.3304
www.hartmanlaw.com

Bradley P. Hartman

June 2010

In the age of computer hacking and identity theft, more and more attention is being focused on the obligation of businesses to protect the security of personally identifiable information stored on its computers and in its databases.

Most businesses retain electronic records containing personal information about employees, vendors, and customers. Does holding that personal information and data create a duty to conceal and protect that information from others on behalf of the person about whom the data relates? Most courts have held that no implied duty exist. If you properly obtain non-confidential data from your employees, customers or vendors, you have the right to use it. The fact that you know your customer's home address and phone number, for example, does not create a duty to keep that information secure. Indeed, the customer's name, address and phone number may be known to many individuals and businesses.

But some employee, customer and vendor information is more sensitive, and may be delivered to your business under confidentiality agreements or under circumstances sufficient to imply a duty to protect the information from disclosure. For example, social security numbers, bank account information, personal health information provided for insurance purposes, and other sensitive data could be used by others for improper purposes. If it is foreseeable that damages could result from the public disclosure of sensitive personal, financial or health information, a business is wise to protect that information to the greatest extent possible.

- **Encrypt.** Current laws generally apply only to "unencrypted personal information." All computer data containing sensitive information should be encrypted and opened only with a password to prevent unauthorized access.
- **Limit.** Business policies and practices should limit access to sensitive data to those individuals with a need to use the particular data in the course of their job duties.
- **Train.** Train employees on the need to secure and protect sensitive data from unauthorized access, including personal information as well as company information, such as marketing plans and strategies, product designs, and manufacturing processes. Additionally, train employees on how to spot unauthorized access to sensitive data so that

your company can be vigilant in identifying data theft and complying with laws that require prompt notice to impacted individuals. Evidence of employee training can help the company avoid a punitive damages award in the event of unauthorized access.

- **Monitor.** Today's network technologies can help you identify unauthorized data access attempts, such as multiple erroneous password entries, access to the database from an IP address or location outside the company, file modifications that evidence copying or emailing of sensitive data, or after-hours access to a secure database.

If your database is ever breached, the worst thing you can do is ignore the breach and hope that no one will find out or nothing will be used improperly. Be warned that there are state and federal laws that require businesses to take specific actions to promptly notify affected individuals and assist those individuals with protecting their financial records and credit rating.

For more information regarding this issue, please contact Brad Hartman (bhartman@hartmanlaw.com) via email or by telephone at 480.659.1515.