

October 2006

# legal update



underberg & kessler LLP

## **Electronic Records: Safe and Secure. What to Do if the Unthinkable Happens**

*By Helen A. Zamboni, Esq.*

More and more firms are becoming increasingly dependent on their electronic records systems. However, moving from paper to computerized records poses a new risk to business owners in addition to the costs associated with system implementation and data migration to the new storage environment – the loss of sensitive customer or employee data.

Almost every business faces the potential, in an era of increasing use of laptops and PDAs, that one of these devices may fall into the hands of an unauthorized person through criminal activity or neglect. Recently, the theft of a laptop computer from the home of a Veteran's Administration employee has made the news.

Another potential for data loss arises as a result of outsourcing your IT support. Your vendor may require you to provide a copy of your database in order to resolve problems with the operation of the system. Use of "test" files is often inadequate to replicate a problem your office staff experiences in actual use of the system, and if a problem can't be replicated, it can't be fixed. Now your sensitive data is not only on computers in your office but also on computers at a location not under your control. Suppose someone hacks into the vendor's system and accesses your files on the vendor's computers or breaks into the vendor's building and steals the computers?

No matter how it happens, if the compromised electronic records contain "personal" or "private" information about your employees or customers, under New York General Business Law §899-aa, you have very specific obligations.

The first thing you must do is notify the potentially affected people that their "personal" and "private" information has been or may have been acquired by an unauthorized person. Note that this means you must make this notification even if you aren't sure whether your files were compromised – unless you know with certainty that they weren't, you must give the notice. The

notice must be made as quickly as possible, consistent with the needs of law enforcement personnel in conducting any investigation of possible criminal activity that lead to the breach.

Under the law, "personal information" is any information, such as a name, which can be used to identify a person. "Private information" means any personal information in combination with any of the following kinds of data elements: Social Security number, driver's license number, credit or debit card number, bank account number.

Your notice must tell the recipients what items of personal and private information may have been improperly accessed, even if not specifically covered by the statute.

Your notice can be given in several ways: in writing, by email or by telephone. You may only use email if you have consent from your customers to communicate with them in that medium (you probably can assume you have the right to communicate with your employees via email). If you call your employees or customers, you should provide your callers a script to follow exactly, and the callers must maintain a log of all calls made for this purpose.

We recommend that you put this notice in the form of a letter and mail it via regular US mail. The letter should describe as completely as possible what you know about how their information may have been put at risk. If the breach occurred through an incident at your vendor's location, restate as exactly as possible what your vendor told you about the incident to avoid any allegations that you damaged the vendor's reputation.

If you can demonstrate to the Attorney General that you have to notify more than 500,000 people, or that the costs of notification will exceed \$250,000, or that you don't have sufficient contact information to reach the affected people by phone or by letter, then you may use substitute notice. This consists of email messages to the people for whom you have email addresses, posting of a conspicuous notice on your website and notification to major statewide media.

You should tell your employees and customers there are steps they can take to protect their identities. The Attorney General's Office has a brochure on its website you may want to download and copy to enclose with your notice. It is available at:

[www.oag.state.ny.us/consumer/tips/identity\\_theft.pdf](http://www.oag.state.ny.us/consumer/tips/identity_theft.pdf)

Finally, your notice must include information on how the recipients can contact you. Obviously, if the affected people are current or former employees, they should be directed to your human resources department. For customers, we suggest you designate specific members of your office or customer service staff to handle customer calls and identify them by name in your notice. It will be helpful to these staff if you develop answers to the questions they are most likely to get from customers. Whether the affected people are employees or customers, you may want to consider setting up a special "hotline" or email address to deal with inquiries, as well as a "Frequently Asked

Questions” page on your website. If you take any of these steps, be sure to include the details in your notice.

If there were thousands of affected people, or if the information that was compromised was of a particularly sensitive nature, or if you believe the security breach may have occurred as a result of human error or negligence in your office, you should consider retaining a risk management consulting firm to advise you and possibly handle individual and press inquiries.

By law, you are also required to notify the Attorney General, the Consumer Protection Board and the State Office of Cyber Security and Critical Infrastructure Coordination. The latter agency has developed a form to be used for this notice, which includes instructions on how to deliver it to these agencies. You can find this form at the CSCIC website at:

[www.cscic.state.ny.us/security/securitybreach/](http://www.cscic.state.ny.us/security/securitybreach/)

You should have your attorney review your notice to be sure it meets the statutory requirements. We would be happy to assist you should you find yourself in this unfortunate but all too common situation. We also recommend that you promptly notify your general liability insurance carrier of the incident.