TLB
Technology Law Bulletin

Spring 2008

a GesmerUpdegrove LLP publication

Hannaford Data Breach May Trigger New Massachusetts Law

by Joe Laferrera
Joe.Laferrera@gesmer.com

On March 17, the Hannaford Brothers supermarket chain announced that "a novel and sophisticated attack" on computers associated with its point-of-sale checkout system resulted in the theft of customers' debit and credit card numbers. The company is aware of 1800 cases of fraud resulting from the attack. This represents a high profile instance of an increasingly prevalent corporate malady: the data security breach.

States have responded, passing laws requiring notification of individuals victimized by such breaches. The first such law, California's Security Breach Information Act (SBIA), took effect on July 1, 2003. Four years later, Massachusetts has joined 38 other states and the District of Columbia in passing legislation requiring such notice. The Massachusetts Act, effective February 3, 2008, builds on other states' laws while adding a few new wrinkles of its own.

"States have responded, passing laws requiring notification of individuals victimized by [data security] breaches."

The Massachusetts law applies to any person, business or governmental agency that owns, licenses, maintains or stores the personal information of Massachusetts residents. Unlike many data security laws, which are limited to those that do business in the state, the Massachusetts Act attempts to reach beyond its borders and has application to anyone using the personal information of Massachusetts residents.

The Act protects the "personal information" of residents, defined to include a resident's name in combination with that person's (1) social security number, (2) driver's license number, (3) state identification number, or (4) financial account, debit or credit card number (with or without any required access codes or passwords) such that would permit access to the resident's account. Legally obtained public information is not considered personal information under the Act. Although the Massachusetts definition may seem broad, some states have gone further to include medical, health insurance and educational data, dates of birth, electronic signatures and biometric and DNA information.

But while the scope of the law may seem objective, it applies a subjective test to determined whether notice must be provided. Specifically, Massachusetts defines a breach of security as "the unauthorized acquisition or unauthorized use of unencrypted data…that is capable of compromising the security, confidentiality, or integrity of personal information…that creates a substantial risk of identity theft or fraud against a resident of the commonwealth." This standard was clearly meant to leave some discretion in the hands of the information holder and does not trigger notice where the risks to Massachusetts residents are remote.

(Data Breach Law, continued from p. 1)

When comparing notification laws, reporting standards vary widely. In contrast to the Massachusetts law, some states have opted for acquisition-based standards which typically mandate at least some form of notice when protected personal information is accessed or acquired without authority. Acquisition-based standards are more rigid than risk-based standards and leave little or no discretion in the hands of the information holder.

The Massachusetts Act also contains a major exception to the notice requirement even if a security breach does occur. Specifically, Massachusetts does not require notice if the data subject to the breach was "encrypted" and that encryption process was not compromised by the breach. This exception is unique in that it requires an encryption process that meets certain technical criterion. In order to rely on this exception, data must be encrypted with "a 128-bit or higher algorithmic process."

In the event of a security breach involving unencrypted data, there are two distinct notice requirements under the law. First, notice must be sent directly to every affected resident in writing or in electronic form. Additional notice options are available if the cost of giving written or electronic notice will exceed $250,000, over 500,000 Massachusetts residents are affected or the party required to give notice has inadequate contact information to do so. These alternative forms of notice include e-mail, "clear and conspicuous" online posting on the information holder's website and publication or broadcast that "provides notice throughout the commonwealth."

Second, written notice of a security breach must be given to the Massachusetts Attorney General and the Director of Consumer Affairs and Business Regulation. This follows a growing trend among states of requiring notice to state agencies.

The content of this notice differs significantly based on the recipient. For example, notice to the state agencies must feature the nature of the security breach and the number of residents affected, while notice to the affected persons "shall not" include this information. At a minimum, Massachusetts residents must be notified of their right to obtain a police report concerning a security breach as well as information about how to place a "security freeze" on their credit report. The "security freeze," which is unique to the Massachusetts Act, allows consumers to limit access to and gain greater control over their credit reports.

In addition to the notice obligations described above, the Massachusetts Act requires proper disposal of personal information about its residents. What is unique about this feature is the specificity of the standard for the destruction of data. Every person and organization covered by this law must ensure proper disposal of records (including electronic records) containing personal information so that they "cannot practically be read or reconstructed." Appropriate methods of data destruction mentioned in the Massachusetts law include having paper documents "redacted, burned, pulverized or shredded" and electronic records "destroyed or erased." Failure to properly destroy records containing personal information could result in fines of $100 per occurrence. Accordingly, those in possession of personal information of Massachusetts residents must have appropriate measures in place.

Data security breach notification laws are becoming increasingly prevalent. Meanwhile, as e-commerce thrives a growing number of companies are maintaining personal information about residents of multiple states. It is imperative that businesses and entrepreneurs know what data they have in their possession so it be managed properly. While the Hannaford situation is still developing, the fallout could be devastating. Sound data management policies limit risk for businesses and protect consumers, and now they are mandatory for those who do business with Massachusetts residents. ♦

MA Court Decision Introduces Dispute About Online Infringement

by Joe Laferrera
Joe.Laferrera@gesmer.com

For several years, the Recording Industry Association of America (RIAA) and record companies have attempted to protect the music industry by aggressively pursuing individuals who make copyrighted music freely available to others over the Internet. To thwart the illegal dissemination of copyrighted music, the RIAA has instituted thousands of lawsuits against people who have offered up music files to so-called peer-to-peer networks, where they can be downloaded for free. With some high profile exceptions, these lawsuits have been largely successful, leading to settlements or favorable verdicts in court.

There is no longer much legal doubt that distributing hundreds or thousands of copies of a song to the public without permission constitutes copyright infringement, but evidentiary and technical hurdles can still make these cases difficult to pursue. First, the RIAA typically requires assistance identifying the infringing parties, since the exchange of files over peer-to-peer networks can be done anonymously. The RIAA only has the "IP" or Internet addresses of the computers involved, and it frequently issues subpoenas to Internet service providers (ISPs) that provide the Internet connections in order to match the IP addresses to actual names. Once a defendant is identified, proving that the songs in question were actually copied by third parties can also be difficult. So, the RIAA has argued that simply making copyrighted music "available" over the Internet is tantamount to copying, and therefore establishes proof of illegal infringement.

On March 31, 2008, United States District Court Judge Nancy Gertner, sitting in the District of Massachusetts, largely rejected the music industry's "access equals infringement" position. Her 55-page decision in *London-Sire Records, Inc. v. Does 1-21* addresses the record company's attempt to compel Boston University to identify the users of certain suspect IP addresses. Judge Gertner granted the defendants' motion to quash the subpoenas, although she left open the possibility of a modified subpoena to address privacy and identification issues.

The most interesting part of the decision, however, concerns the applicability of copyright law to plaintiffs' allegations: whether the defendants have violated the strictures of the Copyright Act, which prohibits unauthorized "distribution" of protected works, by making copyrighted songs freely available on the Internet. Judge Gertner concluded that "merely exposing music files to the Internet is not copyright infringement." She rejected the efforts by the plaintiffs (and some other courts) to equate the defendants' "publication" of the files with their illegal "distribution," stating that "even a cursory examination of the statute suggests that the terms are not synonymous." She holds that "the defendants cannot be liable for violating the plaintiffs' distribution right unless a 'distribution' actually occurred." In short, a college student who made hundreds of music files available over a peer-to-peer network has not violated the Copyright Act until the first download.

This view suggests a departure from several older decisions, and even some recent ones. Indeed, on the day the decision in *London-Sire* issued, the federal District Court for the Southern District of New York reached a contrary conclusion in *Elektra Entertainment Group, Inc. v. Barker*, stating that "Several courts (including the Supreme Court) that have wrestled with the Copyright Act have generally found…'distribution' and 'publication' to be synonymous."

Whether, and how, the courts reconcile this issue is still unclear. But until they do, the music industry may find some places far less hospitable than others when pursuing their lawsuits.♦

GesmerUpdegrove LLP
40 Broad Street, Boston, MA 02109

Return Service Requested

© 2008 Gesmer Updegrove LLP. All rights reserved. This may be considered advertising under Mass. R. Prof. C. Rule 7.3(c).