



Into the Data Breach Law (Kevin M. Lemley Commentary)

By Kevin M. Lemley - 5/28/2007

Arkansas recently enacted the Personal Information Protection Act to govern data security. The act requires that any business with personal information of an Arkansas resident to take reasonable measures to protect that information. The law applies to both the company compiling the information and any data company storing the information.

The law does not define "reasonable measures"; the boundaries of that phrase will be forged in the courts through the inevitable lawsuits to be filed.

For purposes of the act, "personal information" consists of the person's name combined with one or more of the following: account number or credit/debit card number in combination with any required security code; Social Security number; driver's license number; Arkansas identification card number; or medical information. The act requires disclosure if unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. However, notification is not required if the firm conducts a reasonable investigation and determines there is no reasonable likelihood of harm to customers. Individuals or the Attorney General can file a lawsuit under the act. Additionally, Arkansas firms may be subject to other states' laws, many of which have stricter standards than Arkansas'.

The effects of the act are unclear because the data breach litigation front is still developing. The first wave of lawsuits, like *Bell v. Acxiom* in Arkansas, claimed the data breach alone caused harm. These lawsuits were promptly dismissed. The second litigation wave focuses on data breach notice and situations where actual harm was inflicted. In California, a class action was filed against General Electric when an employee lost a company laptop that contained the personal information of 50,000 employees. Although GE issued a notice pursuant to California law, the complaint argued the notice was inadequate. The plaintiff dismissed the case in March, presumably on the heels of a handsome settlement.

T.J. Maxx has been hit with two consolidated class actions in Massachusetts federal court -- one by a class of consumers and one by numerous financial institutions. The financial institutions alone are seeking tens of millions of dollars. The lawsuit is based on failure to reasonably protect information; Massachusetts does not have a data breach notice law.

No case has been filed yet under Arkansas' new law, but these recent lawsuits show that Arkansas firms are threatened with three basic types of lawsuits: failure to reasonably protect data, failure to provide notice of data breach and inadequate notice.

The lawsuits will likely come in the form of class actions consisting of customers, employees, business partners and even the Attorney General. Like TJ Maxx, Arkansas firms can quickly find themselves fighting a multi-front legal war while desperately trying to retain their customers. The added litigation compounds the extensive costs of a data breach. Even without a lawsuit, the Ponemon Institute estimates an average data breach costs \$4.8 million per incident. Darwin Professional Underwriters provides a free online calculator that generates similar results.

Several precautionary steps can minimize the harm caused by a data breach:

- Avoid the requirements of mandatory disclosure under the act. This can be accomplished by encrypting data or storing data in a disconnected manner that it is not considered "personal information." By doing so, the firm can eliminate claims for failure to provide notice or for inadequate notice.
- Consider procuring data breach insurance coverage. At least two insurers currently provide such coverage: Darwin Professional Underwriters and AIG Corporate Identity Protection.
- Identify the strictest state law the firm is subject to and adopt a policy that will meet that law.
- Consider issuing a data breach notice even if not required by the act. The Ponemon Institute found that 82 percent of consumers feel a notice should be sent even if not required by law.
- Issue personalized communications in the event of a data breach. Customers who receive personalized communications are three times less likely to terminate their relationship than when they receive an impersonal mass communication. After all, protecting and maintaining your customers is the top priority when a data breach occurs.

(Kevin M. Lemley is an attorney with the Allen Law Firm in Little Rock. E-mail him at kmlemley@allenlawfirm.com.)

Copyright © 2007, [Arkansas Business Limited Partnership](#). All Rights Reserved.