IT Pays to Be Prepared: The Cost of Data Breaches

Failure to Properly Guard Information May Carry a Hefty Price Tag Regardless of Whether an Actual Injury Resulted

BY THOMAS E. ZENO AND LINDSAY HOLMES

As a result of holiday hacking into the computer systems of major retailers like Target and Neiman Marcus, millions of customer names, account numbers, PINs, addresses, telephone numbers and email addresses have been compromised. What will these security breaches cost? Some say very little, adding that lower security precautions during high-traffic shopping seasons are worth the risk. In December, Target and luxury retailer Neiman Marcus were both the target of hackers that breached the companies' systems and stole millions of credit card records. Those who followed the result of the recent settlement in the AvMed litigation may think differently. Companies failing to pay for data security will face calls to repay their "unjust enrichment." The answer is that ***IT*** (information technology) pays to be prepared for a data breach. Now is the time to implement data security measures that will protect your company and your customers in the future.

In 2009, AvMed, a Florida-based health insurer, reported the theft of two laptops containing unencrypted personal information of more than 1.2 million customers, including names, Social Security numbers and health-related information. Class-action litigation began in 2010, and the parties entered into a settlement agreement in October 2013. The agreement requires AvMed not only to implement the data security measures it should have had in the first place—such as security awareness training, upgraded laptop security systems, and upstaged security policies and procedures—but it also requires AvMed to forfeit the "unjust enrichment" it has received over the years by not spending sufficiently for the data security it should have provided. Thus, without proof of actual harm to the individual, such as identity theft, AvMed is required to reimburse customers for a portion of their premiums. It's unclear whether unjust enrichment claims will be successful in actual litigation, but the approach has been given added vitality through the AvMed settlement.

Although experts predict that data losses are likely inevitable, damage to your organization does not have to occur. Lost or stolen data does not automatically become a data breach. In many cases, simple steps such as encryption would have rendered the stolen information unreadable and no breach would have occurred. Many of these steps are already considered standard practice.

Data Security Standards

Whether your organization handles personal information now, or may do so in the future, federal and state laws are likely to set the standard by which unjust enrichment claims will be made and damages calculated. The following is a non-exhaustive list of examples of what those standards expect.

Federal

The Federal Trade Commission (FTC) polices "financial institutions" subject to the Gramm-Leach-Bliley Act (GLB Act). Businesses that significantly engage in providing financial products and services are required to protect the security and confidentiality of information they collect, such as names, addresses, phone numbers and credit card information. The FTC has issued the

Safeguards Rule pursuant to the GLB Act that requires measures to keep consumer information safe. These protections require implementation of an information security program that can include a written security policy, ongoing monitoring, security training, access controls, background checks, laptop and cell phone policies, employee sanction policies, termination procedures, and so forth.

The FTC has also been involved in data breach enforcement by alleging "unfair and deceptive trade practices" against companies that did not properly protect consumer information leading to identity theft. As of 2011, the FTC had brought more than 30 cases against a range of companies for violations of consumers' privacy rights or for data breaches. A number of the settlement agreements require periodic audits during the next 20 years, implementation of security programs and civil monetary penalties.

State

Currently, 46 states as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have data breach notification laws, some of which are broad enough to span multiple industries. For example, Massachusetts state law requires notification by any "person or agency that maintains or stores … data that includes personal information about a resident of the commonwealth" when it "knows or has reason to know of a breach of security or" the information "was acquired or used by an unauthorized person or for an unauthorized purpose." Personal information, as defined by Massachusetts law, can be the first initial and last name of an individual coupled with a social security number, driver's license number or credit card number. Based on the broad definition of personal information, this and other state laws should prompt all companies to properly protect customer information.

Industry

Industry has also been influential in setting standards for interaction with consumer personal information. The Payment Card Industry Data Security Standards (PCI DSS)

provide guidelines for handling cardholder information. The standards are comprised of security incident prevention, detection and response processes. They include data security activities such as monitoring security controls, detecting and responding to security control failures, accessing gaps in protection and annual inventory reviews.

Best Practices

By maintaining awareness of applicable data security standards and following industry best practices, your company can help avoid the fate of falling victim to data breaches. Here's a non-exhaustive list of practical tips for protecting data held by your organization. Many of these suggestions are also encouraged by ALTA's "Title Insurance and Settlement Company Best Practices." For more on ALTA's Best Practices, go to *www.alta.org/bestpractices*.

Organize Your Data

Determine where personal information is stored and who has access to it. Ensure that wherever personal data is kept, it is secure and segregated from other information. All personal data that is not necessary to business operations should be properly destroyed.

Establish Updated Policies and Procedures

Policies and procedures covering privacy and security should be tailored to your organization. Policies should anticipate a variety of issues include texting, use of social media, BYOD (bring your own device), cloud storage and use of external storage devices (e.g., external hard drives and thumb drives). It is important to update these policies and procedures to meet the changing technology and business environment.

Encryption

Use encryption as specified by the National Institutes of Standards and Technology, especially on portable devices that store protected information (e.g., laptops, memory sticks). Additionally, keep your encryption key separate from the device.

Computer Security Protections

Common computer security protections can go a long way in protecting personal data. Examples include installing software patches, requiring robust passwords, requiring multiple-factor authentication for remote access and terminating dormant accounts. An overlooked precaution is keeping an up-to-date inventory of the equipment in the organization, ranging from mainframes to backup tapes.

Limiting Access

Limiting access to data and technology not only reduces the opportunities for a breach, but it also restricts the potential damage if a breach occurs. Such limits can include controlling employee access to certain websites (so as to avoid hacker sites), regulating employee access to data storage (on an as-needed basis) and establishing an employee exit procedure (including an exit interview and separation agreement).

Employee Training

Policies and procedures must be shared throughout the organization. This can be accomplished through employee training sessions on general topics such as proper privacy and security procedures as well as on specific risks for breach identification and the appropriate response. These sessions should be updated and repeated on a regular basis. New employees should be trained promptly upon being hired.

Conclusion

It is no surprise that companies are feeling the financial pinch of upgrading data security systems to assure that they do not fall victim to hackers, thieves and even unintentional errors resulting in loss of protected information. Some organizations have reasoned that the time and money necessary to implement data security measures are not worth it. AvMed would likely disagree.

Although proving the causal link between the breach of consumer information and an injury can be difficult, the theory in the AvMed case will make damages easier to determine. The standard of due care is likely to be established by federal and state data privacy laws. Going forward, an organization's failure to guard information properly may carry a hefty price tag regardless of whether an actual injury resulted. The money an organization thinks it is saving, may in fact, be nothing more than "unjust enrichment." ■

Thomas E. Zeno, a former assistant U.S. attorney for the District of Columbia, is now Of Counsel to Squire Sanders. He can be reached at *thomas.zeno@squiresanders.com*.

Lindsay Holmes is a fellow in Squire Sanders' Washington, D.C., office. She can be reached at *lindsay.holmes@squiresanders.com*.