Spotlight On: Consumer Financial Services

Heartland Data Security Breach Highlights the Need for Uniformity, Transparency in Consumer Notification Rules

Written by:
*Jennifer Rossi, Mathew Jasinski & John Tanski**

January 26, 2009

In what may be the largest data security breach ever reported, Heartland Payment Systems, Inc., a credit card processor based in Princeton, New Jersey, announced on Tuesday that cyber criminals wielding sophisticated malware had hacked into its computer network, gaining access to tens of millions of credit card records.

Although the details have not been fully disclosed, what we know now of Heartland's data security breach highlights the shortcomings of the status quo. Heartland is based in New Jersey, but its customers include restaurants and small retailers in all 50 states. In processing 100 million credit card transactions each month, Heartland acquires private data-such as names, addresses and credit card numbers-from millions of consumers across the country.

Commentators have questioned the disclosure's timing, suggesting that Heartland deliberately chose Inauguration Day as a way to bury the story. Regardless, Heartland's data breach provides the Obama administration with an opportunity to protect the privacy of American consumers and provide needed uniformity and clarity to businesses. National legislation in this area is overdue.

State Data Security Laws

In 2003, California blazed a legislative trail when it became the first state to adopt a data breach notification law. Currently, 44 states, the District of Columbia, Puerto Rico and the Virgin Islands require notification of security breaches involving personal information. Undoubtedly, many were motivated to act by data aggregator ChoicePoint's February 15, 2005, disclosure that identity thieves had compromised ChoicePoint's database, stealing the personal information of 145,000 people.

California's data breach law defines "personal information" as a person's first name (or first initial) and last name, together with his or her social security number or driver's license number, or account number if the account number is accompanied by data-such as a security code or password-that would permit access to that account. Some states and jurisdictions have adopted this definition. Others have gone further to include one's date of birth or mother's maiden name.

The differences among the laws do not end here. Notably, California and several other states and jurisdictions require notification to affected individuals irrespective of the risk of actual harm. Some, on the other hand, require notification only if the breach will likely result in harm. Other differences include how and when to notify persons whose personal data has been compromised, whether those persons can file suit if the business fails to notify them properly, and whether state agencies and municipalities must comply with the notification requirements.

In addition, many states also have adopted laws that permit consumers to freeze access to their credit reports, and the latest trend is to require those who collect Social Security numbers in the course of business to create and display privacy protection policies. Connecticut's privacy law, which became effective last October, has a significantly broader reach than that state's breach notification law; it applies to all "information capable of being associated with a particular individual through one or more identifiers."

This lack of uniformity leaves a national firm like Heartland in a bind while needlessly driving up compliance costs. Moreover, each state and jurisdiction has its own mechanisms for

enforcing its data breach laws, meaning that Heartland may face a consumer class action in one state, an attorney general investigation in another, and both in a third. The cost of defending against multiple actions in multiple jurisdictions under multiple laws is a deadweight loss in a system that has 47 similar but distinct ways of achieving the goals of preventing data security breaches and providing prompt and fair notice to consumers when a breach occurs.

Data Security at the Federal Level

Soon after California passed its landmark data breach notification law, that state's senior senator, Dianne Feinstein, introduced a similar bill in Congress. Since then, dozens of measures have been proposed at the federal level with the hope that federal legislation will result in some measure of national uniformity. The timing is right for Congressional action.

Senator Feinstein's bill, the Data Breach Notification Act-which she reintroduced at the beginning of the 111th Congress-would supersede all federal and state rules regarding data breach notification, at least with respect to companies doing interstate business. Although based on California's landmark statute, Senator Feinstein's bill adopts the more moderate approach taken by many states, requiring notification only when there is a risk of harm to consumers.

However, the bill does retain a somewhat ambiguous requirement that consumers be given notice of a data breach "without unreasonable delay." It also fails to define the key term "sensitive personally identifiable information." These shortcomings still would leave businesses in the dark about what is expected of them, but at least they would be in the same room. Courts would be left to interpret one statute, not forty-seven.

That said, it bears repeating that, as its name suggests, the Data Breach Notification Act occupies only the field of breach notification, not breach prevention. Uniformity is needed in this arena as well. By way of example, a controversial Massachusetts regulation scheduled to become effective in May has onerous encryption obligations and would apply to untold numbers of regional, national and international companies, charities, and colleges and universities. Other states may follow suit.

Enforcement and Litigation

By and large, state attorneys general are responsible for the enforcement of the existing state data security statutes, and Senator Feinstein's bill also would grant them enforcement authority. They would share it with the U.S. attorney general, however, who would have the power to remove any case to federal court. Although her bill would not permit consumers to bring individual or class action lawsuits for federal data breach law violations, it would not stop them from suing on other theories, such as negligence.

Whether state or federal, legislation comprises only part of the data security landscape for businesses such as Heartland. Litigation is a blunt but effective tool for redressing unnecessary data retention, inadequate data protection, and incomplete data destruction. Businesses also risk FTC enforcement. That agency frequently alleges that data security breaches constitute "unfair acts or practices," based on the failure to take "reasonable security measures" to protect consumer data. Some scholars have questioned the FTC's authority to do this, but its targets have not tested the agency's authority. They've settled.

Before Heartland, the largest retail data security breach involved discount retail giant TJX and the theft of 45 million customer credit and debit card numbers. Although TJX disclosed the breach in early 2007, much of the theft occurred in 2003, before the vast majority of today's data security laws. Nevertheless, TJX faced an FTC enforcement action, a barrage of consumer class actions claiming negligence, breach of contract and violations of Massachusetts' unfair trade practices act, and lawsuits brought by financial institutions alleging similar claims in a bid to recover their costs associated with related fraudulent credit card purchases.

Conclusion

Since TJX, state legislators have been busy, and Heartland could potentially bear the brunt of 47 overlapping and, at times, inconsistent statutes. Given the need for uniform data breach notification requirements, as well as consistent prevention measures, it is time for federal action. In the meantime, businesses that collect personal information must do their best to comply with the existing morass of laws. In the struggle to untangle this legal web, however, one must not lose sight of its purpose: to prevent and contain data security breaches. The pace of technology outpaces that of legislation, and the marketplace will come to dictate-if it has not already-that businesses not merely comply with these measures but rather lead the way.

The information in this spotlight should not be considered legal advice. Consult your attorney before acting on anything contained herein.

* Attorney Jennifer R. Rossi leads the Consumer Financial Services Team in the Business Litigation Practice Group at Robinson & Cole LLP. Team members, Attorneys Mathew P. Jasinski and John M.Tanski, assisted Ms. Rossi in writing this article. Ms. Rossi can be reached at jrossi@rc.com or (860) 275-8200.