LAW | REAL ESTATE | FINANCE
DailyBusinessReview.com
An ALM Publication JANUARY 29, 2014
DAILY BUSINESS REVIEW

SPECIAL REPORT: DATA SECURITY

Data security—Legal risks to watch out for in 2014

Commentary by Al Saikali

The data security legal landscape is changing quickly, which can be exciting for lawyers, but unpredictable and scary for companies trying to measure and minimize the risks. This article discusses three areas that I recommend all in-house lawyers and corporate executives should monitor in 2014.


Saikali

When a company suffers a data breach, its notification obligations are governed by a patchwork of 46 state laws, federal sector-based laws, international laws and contractual obligations. The law that applies to the breach is the law of the jurisdiction where the individual whose information was compromised resides.

So when an employee loses a laptop containing personally identifiable information for thousands of individuals, chances are all 46 state data breach notification laws are in play, which can be expensive and confusing for a company that does not use experienced counsel. Some similarities between the laws exist, but they often differ on how soon a company must issue notification, who it must notify, and how it must notify.

A federal data breach notification law would go a long way to resolving some of this uncertainty. Until recently, all attempts in Congress to enact such a law failed due to state concerns about preemption and lack of federal resources to enforce such a law. The high-profile nature of the Target data breach appears to be affecting the legislative environment, with Congress now holding hearings to understand how to better protect consumers when data breaches occur, and data breach notification laws being introduced for consideration.

But some unanswered questions remain regarding the proposed federal legislation: How quickly will companies have to notify of a data breach, and will the law give companies time to understand and remedy the breach? What role will regulatory authorities play in enforcing the law? Will the law allow for private causes of action? Will state breach notification laws be preempted? It will be important to monitor what relief companies obtain from the federal government in the form of a data breach notification law that tries to unify the existing patchwork of state laws.

PRIVATE CLASS ACTIONS

On the litigation front, I'm watching two big issues in 2014: liability arising from data breaches and liability arising from companies' failure to adequately disclose what information they collect about consumers and how

they use that information.

Until recently, plaintiffs have not experienced much success with class action lawsuits against companies that have suffered data breaches. Courts usually conclude the plaintiffs lacked standing and suffered no real damages or cognizable harm.

Nevertheless, a few recent cases, including two filed in the Southern District of Florida, have resulted in favorable outcomes for the plaintiffs and should give corporate organizations pause for concern.

In one case, two unencrypted laptops were stolen from a company's conference room. The laptops contained personally identifiable information for approximately 1.2 million individuals. The plaintiffs filed a class action lawsuit that the trial court dismissed on the ground that the plaintiffs had not suffered any cognizable injuries. The appellate court disagreed and allowed the lawsuit to proceed, reasoning in part that the plaintiffs had paid premiums to the company, and a portion of those premiums was for administrative services (including securing the customers' information), and the plaintiffs were entitled to pursue that small portion of their premiums as damages. The case settled for approximately $3 million, demonstrating the importance for any company to have a strong information security plan in place.

In another Southern District of Florida case, a company shared personal information about its employees with a vendor whose employee misused access to that information to engage in identity theft. The trial court denied a motion to dismiss, and the case subsequently settled for more than $400,000. How companies manage their vendors could be a big source of liability in 2014.

A federal appellate court also recently held that plaintiffs in a data breach class action were entitled to seek damages in the amount of credit monitoring, card replacement and other mitigation expenses. Plaintiffs in lawsuits across the country are citing that opinion in response to arguments that they didn't suffer cognizable damages.

Whether these cases are outliers or the beginning of a new trend in favor of plaintiffs remains to be seen. The Target data breach litigation will be a good test of this emerging precedent.

The second area of litigation to watch in 2014 is class action lawsuits that arise from companies that collect and use information about individuals without adequately disclosing those collection and use practices. Most companies have privacy notices on their websites or in their mobile apps that describe what information they collect about consumers (names, email addresses, certain financial information), but oftentimes the apps collect additional information (location, IP addresses, etc.), and the notices unintentionally do not disclose the collection of this additional information. We can expect to see civil lawsuits very soon based on these failures to match privacy notices with actual practices.

REGULATORY ROLE

Another area to watch in 2014 is the role of regulatory authorities. The FTC Act gives the Federal Trade Commission the authority to pursue companies that engage in unfair or deceptive trade practices. In the world of data security, this means enforcement in three ways: Did the company adopt reasonable safeguards to secure consumers' information before the breach, did the company timely notify affected individuals after the breach and are companies adequately disclosing what information they are collecting from their consumers and what they're doing with that information.

A couple of companies are fighting back, arguing the FTC is acting beyond its authority by judging the reasonableness of a company's security safeguards after-the-fact. I suspect the FTC will likely defeat those challenges, which could further embolden regulatory enforcement after data breaches are made public.

In addition to the FTC, many state attorneys general regularly investigate data breaches. Some state data breach notification laws require companies to notify their respective state AG about the breach, which can result in an inquiry as to what caused the breach, what protections were in place to prevent it and how the company responded to it. Increasingly, the AGs are coordinating their response to notification of data breaches, but we should expect to see them remain active and bring enforcement actions where appropriate.

Finally, companies should watch how the U.S. Department of Health and Human Services' Office of Civil Rights enforces recent changes to the Health Insurance Portability and Accountability Act's privacy, security and breach notification rules. The changes were part of the final omnibus rule, which now creates a presumption of a breach where there was a use of unencrypted protected health information, or PHI, that is not a "permissible use" under HIPAA. Examples would include the viewing of PHI by an unauthorized third party or the loss/theft of mobile devices containing PHI. Importantly for companies not in the health sector, the final omnibus rule reminds us that HIPAA applies to companies that do business with health care providers and share PHI in that business relationship, so law firms, cloud service providers and other companies that service healthcare providers should monitor how HHS is enforcing the final omnibus rule.

In conclusion, the legal landscape for data security is changing rapidly as companies increasingly collect, store, use and dispose of sensitive electronic information. Companies must monitor these changes and stay ahead of the curve so they don't find themselves on the wrong side of a data breach lawsuit or regulatory inquiry.

Al Saikali is a partner in the Miami office of Shook, Hardy & Bacon, where he co-chairs the firm's data security and data privacy practice group. His email address is asaikali@shb.com.