CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 159 years

THURSDAY, MARCH 27, 2014

Chicago Daily Law Bulletin®

Volume 160, No. 61

Many lessons for companies to learn after the Target data breach

The red bull's-eye. Even shoppers that don't frequent Target know the retailer's ubiquitous logo.

But what many holiday shoppers — both loyal Target customers and casual visitors to the trendy discount store — didn't realize until too late was that swiping their credit and debit cards at Target registers painted another kind of bull's-eye — this one on their backs.

In mid-December, a security researcher and technology blogger revealed that, around the time of Black Friday, Target had suffered a massive data breach "potentially involving millions of customer credit and debit card records" and leaving those customers at risk for fraud and identity theft.

Caught off guard by this public outing, the company scrambled to control the situation on multiple fronts, investigating the breach, dealing with panicked customers and managing the mounting PR crisis.

This is the first in a two-part series analyzing the Target data breach. This piece will analyze Target's missteps in handling the breach and offer some suggestions for how companies should handle data breaches such as these.

The second part will analyze why the breach happened and how Target could potentially have prevented the breach.

Target's response to the public revelation of the data breach

After the public outing of Target's data breach by a tech blogger, Target Chairman and CEO Gregg Steinhafel apologized, saying that the company's "first priority is preserving the trust of our guests," and that it would swiftly address the cause of the breach, which apparently took place over a three-week period, from Nov. 27 to Dec. 15. Initially, Target reported that 40 million credit and debit card numbers had been compromised.

Then, Target discovered that another 70 million people had their personally identifiable information (names, phone numbers and e-mail addresses) stolen. Reportedly, Steinhafel was advised not to disclose the second breach; his advisers argued the second breach did not require disclosure because it did not involve financial information.

Steinhafel, in an attempt to be as transparent as possible, decided to disclose the breach. Some commentators have argued that this second disclosure was Target's undoing. It annihilated the public's remaining trust in Target because it appeared as if Target had neither control of the situation nor an understanding of the scope of the breach. The media also focused on the size of the breach, creating the mantra that it affected "a third of the American public."

The rapid succession of these additional breaches suggests more data breaches are inevitable. The question is not whether a company will suffer a data breach, but when.

Jeffrey Jones, Target's chief marketing officer, reportedly lamented that the public "keeps hearing that (the number of people affected by the breach) equals one third of all Americans. That's hammering us."

Damage to Target

The financial toll of what some are calling the "worst data breach in American retail history" is astronomical.

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a partner in Loeb & Loeb's Chicago office. She focuses on matters involving the convergence of advertising and promotions, emerging media, technology and privacy law as well as intellectual property law. She can be reached on nmcginn@loeb.com.

According to the retailer, the data breach resulted in $17 million of net expenses in the fourth quarter — $61 million total expenses related to the breach were partially offset by $44 million in insurance coverage.

The company has said that it can't yet estimate how much more the data breach will cost. Additional expenses may include payments to card networks to cover losses and expenses for reissuing cards as well as costs related to pending lawsuits, government investigations and enforcement proceedings.

At least one analyst has suggested that the cost to cover only the fraudulent charges to the breached cards may reach somewhere in the neighborhood of $1.4 to $2.2 billion — of which Target would be responsible for $400 million to $1.1 billion.

In addition to these losses, the breach also has damaged Target's profits and brand.

On Feb. 26, Target reported that it earned $520 million for the three months that ended Feb. 1, a sharp decline from the previous year's profit of $961 million.

The breach also has hit Target's stock value. Before the company's release of its most recent revenue numbers, Target shares were valued at $57.60, a full 10.5 percent lower than its share price of $63.50 just prior to the revelation of the data breach.

Target's legal nightmares

In addition to the escalating financial costs and reputational damage, Target now must defend itself against a national wave of lawsuits.

The company is facing numerous consumer class actions alleging that it failed to adequately protect customers' data and seeking compensation for long-term credit- and identity-theft monitoring for customers as well as suits by banks and other financial institutions seeking compensation for the cost of reissuing cards and monitoring bank accounts for fraud.

In addition, a shareholders' derivative suit against the company's directors and officers alleges that they breached their duties of loyalty and good faith by allowing the company to release false and misleading statements — including statements about the scope of the breach — by failing to properly oversee Target's business and operations and by failing to prevent certain corporate representatives from taking such illegal actions.

Therefore, Target's damages stem not only from the breach itself but also from the handling of the breach.

Likelihood of more breaches

Unfortunately for consumers and American businesses alike, the Target breach is only one of

several recent data breaches that caught the public's attention.

Luxury department store Neiman Marcus has reported a breach involving 350,000 credit and debit cards. White Lodging Services Corp. (which manages hotel franchises for Hilton, Marriott and Starwood hotels) recently announced a suspected data breach involving 14 of its properties and extending over the course of nine months last year.

And national arts and crafts retailer Michaels has announced an investigation into a potential data breach affecting payment cards. The rapid succession of these additional breaches suggests more data breaches are inevitable. The question is not whether a company will suffer a data breach, but when.

Lessons learned from the handling of the Target data breach

The Target data breach offers several important lessons for handling a data breach.

• Be sure to assess the type of information involved in the breach. Depending on the type of information involved, the breach may not have to be disclosed.

• Be sure to assess the scope of the breach. Communicating the wrong information or too little information can be even more damaging than not making any announcement at all.

• Control the timing and the content of the message. The company should reveal the existence of the data breach. By controlling the message, you can attempt to control the media coverage and its inevitable effect on consumer opinions.

Over the years to come, commentators will continue to review and analyze the Target response to this data breach.

While we still have many lessons to learn from how it was handled, by learning these simple lessons we can hope to avoid at least some of the mistakes made by Target.