Privacy Alert - Data Security Breach at Target is an Important Lesson for All Companies

December 20, 2013

News about the data security breach at Target is rapidly developing. Current reports indicate that in the last few weeks, the credit and debit card information for as many as 40 million Target customers was compromised.1 The compromised data apparently includes customer names, credit card numbers, expiration dates, and CVV verification codes—everything a criminal would need to create counterfeit cards.

Given the size and scale of this breach, sophisticated cybercriminals almost certainly are to blame. As the story continues to unfold, it will be interesting to learn whether rogue Target insiders also were involved. Realizing the value that this kind of data brings on the black market, cybercriminals are expanding their focus from traditional targets like health care, financial services, and energy to all kinds of industries, including hospitality, retail, software, and others. And, in order to facilitate their efforts, these criminals are increasingly recruiting insiders to do their dirty work.

While cybercriminal attacks from the outside may seem like a remote possibility to some, no modern business is immune from the risks of a data security breach. For example, a recent study concluded that from June 2012 to July 2013, more than 10,000 laptops, smartphones, tablets and other personal electronic devices were reported as lost in just seven airports around the globe.2 If these devices contained confidential trade secrets or private customer data collected by a company that was not properly encrypted or protected, the real damages and the reputational harm to the company could be devastating.

Create a Risk Management Strategy to Minimize the Harm of a Potential Data Breach

There are a number of steps that companies of all sizes should consider taking in order to reduce the risk of a data breach and contain the harm that could flow from a breach.

First and foremost, companies should be mindful of the sensitive data in their possession, where that data is stored, and who has access to it. Examples of sensitive data obviously would include customer names, addresses, email addresses, and credit card numbers. It also may include confidential business information and trade secrets.

Second, companies should ensure the data they collect is necessary for business operations. Extraneous data should not be collected, and data that is no longer used should be discarded.

Third, companies must make sure that they protect the data they collect and maintain. Only employees who have a legitimate business need for sensitive data should have access to it, and that data should be secured at various points as it travels through a company. When data is discarded, processes should be implemented to make sure the process is done safely. For example, if employees are allowed to bring their own devices (e.g., smartphones, tablets, etc.) to work, company policy must allow for a complete wipe of the employee's device at the company's discretion.

Fourth, companies should review the representations they make to customers and business partners and ensure that it complies with those representations. Statements companies make about how they collect, protect, and share customer information must be truthful and accurate.

Fifth, companies should regularly review their policies and procedures and tailor them to conform with the current business, technological, and legal environment. Terms of Use and Privacy Policies must be current and accurate, taking advantage of any safe harbors or available protections. Data protection systems also must be monitored to ensure compliance with company policies, and employees should receive periodic training on these policies and the importance of data security.

Finally, because the worst time to create any kind of response plan is during a state of crisis, it is critical that companies adopt a data breach response plan before a breach occurs. Advance planning is necessary to quickly identify the nature of the breach and to contain and mitigate the resulting harm. The plan also must include a process for notifying the victims of the breach, as required under state notification requirements and other applicable laws.

A data breach response plan also should consider how the company will deal with media inquiries. The reputational harm that flows from a data breach may be as great as or greater than any civil penalties or damages the company is required to pay. A swift and strategic public relations team can significantly mitigate reputational harm, but advance planning is necessary.

GPM has a team of attorneys who are available to help companies navigate these increasingly scary waters. Our team regularly performs data audits and risk assessments, which we use to help companies develop data privacy and security policies that fit their needs and reflect best practices. Our primary goal is always to help companies avoid data breaches before they occur—but in the event of a data breach crisis, it is critical to have a plan in place that can be executed quickly and efficiently in order to minimize the consequential damage.

[1]See Millions of Target customers' credit, debit card accounts may be hit by data breach, available here.
[2] See AirportLostandFound.com Releases 2013 Statistics—10,000 lost laptops, phone and tablets, available at: www.prweb.com/releases/2013/8/prweb11069359.htm

This article is provided for general informational purposes only and should not be construed as legal advice or legal opinion on any specific facts or circumstances. You are urged to consult a lawyer concerning any specific legal questions you may have.