Target's recent win provides guidance for cybersecurity discovery

November 20, 2015

Just shy of the second anniversary of its massive data breach in 2013, Target remains embroiled in litigation. Battling two separate lawsuits – one brought by consumers, the other by financial institutions – the retailer has faced its fair share of legal woes in the last two years. In September, Target was dealt another blow when a federal judge in Minnesota allowed a class action lawsuit of banks and financial institutions to proceed. However, the company recently scored a discovery victory in the class action suit, one that has important takeaways for other organizations looking to protect breach response materials.

Shortly after the 2013 breach occurred, Target's in-house and outside attorneys established a "Data Breach Task Force" to launch an investigation to determine Target's legal obligations. Specifically, the Task Force was intended to educate Target's counsel on the breach and allow them to provide legal advice and defend the company in pending litigation. At the same time, Target conducted its own ordinary-course investigation, engaging a team to conduct a separate investigation on behalf of credit card companies. Target stated that this investigation was designed to determine how the breach happened and how the retailer and credit card companies could appropriately respond.

Through discovery, the financial institutions sought materials created in the course of both investigations. Target provided a majority of documents related to its own investigation but asserted attorney-client privilege and work-product claims as to the Task Force investigation. The plaintiffs challenged Target's claims of privilege on the basis that Target would have been obligated to investigate and fix the data breach regardless of any litigation.

The court ruled largely in favor of Target, agreeing that the documents related to the Task Force were protected from disclosure. Specifically, the court held that the primary purpose of the Task Force and its investigation was to obtain or provide legal advice. Target's internal investigation, which was focused on remediation, was subject to disclosure, as it was conducted for business, rather than legal, purposes.

This ruling is a good reminder of the need for careful legal planning in advance of data breach incidents. When a data breach occurs, it is important to investigate and gather information to determine an appropriate response, particularly from a legal standpoint. Organizations can take a few clues from Target's win to help protect such information from discovery in the event litigation occurs.

1. Plan In Advance. All organizations should, at a minimum, have a basic data response plan in place. The response plan should be drafted in a way that heavily involves counsel from the beginning. Giving advance thought to the structure of the investigation will help to preserve privilege and allow for a quick response immediately following a breach.

2. Clearly Define The Purpose. It is crucial when initiating or engaging an investigative team that the team's role be clearly defined.

3. Document, Document, Document. Members of the investigative team should describe (in writing) the nature of and reason for the investigation and the involvement and direction of counsel.

4. Educate The Team. Both the organization and the investigative team should be informed as to the privileged nature of the materials and all involved individuals should be counseled on the importance of taking sufficient precautions to maintain the privilege.

5. Keep It Separate. Target was successful in protecting the Task Force documents because of its two-track investigative approach. Much of the information requested by the class action plaintiffs was contained in the documents Target did disclose from its own investigation, and thus it was unnecessary for Target to also turn over documents from the Task Force.

If you have questions about this ruling, please contact Megan Knox (mknox@bricker.com, 614.227.8885) or any member of the Cybersecurity group.

Authors