Akin®

Is Your Privilege On Target? Lessons in Protecting Privilege from the Target Data Breach

Nov 30, 2015

Reading Time : **2 min**

By: Natasha G. Kohne, Anthony T. Pierce, David S. Turetsky, Visiting Professor, College of Emergency Preparedness, Homeland Security, and Cybersecurity at the University of Albany

On October 23, 2015, the district court overseeing the class action litigation relating to the consumer data breach at Target issued an order that denied several challenges to Target's assertions of attorney-client privilege over documents generated in connection with an investigation of the breach. The *Target* court's rationale is instructive for companies formulating their own procedures in the event of a similar breach.

In mid-December 2013, a vulnerability in Target's system allowed hackers to gain access to consumer credit and debit card information. After Target announced the breach, several lawsuits were filed. In early 2014, Target established a Data Breach Task Force to assist its attorneys in investigating the breach. Target's outside counsel also engaged a team from Verizon Business Network Services ("Verizon") to further inform its legal advice to the company.

Target withheld, as privileged, certain communications that it had with its Data Breach Task Force and others with Verizon. The plaintiffs moved to compel these documents, arguing that they were not privileged because Target needed to undertake the investigation to protect itself against future breaches, even if there had been no lawsuit.

The court generally disagreed. It found that Target had conducted an effective two-track investigation into the breach. On one track Target conducted an "ordinary-course" investigation, focused on learning what caused the breach and how it could be remediated. Independent of this investigation, Target "established its own task force and engaged a

separate team from Verizon ("Privileged Verizon") to provide counsel with the necessary input" to help protect the company's legal interests. The court noted approvingly that separate teams did not communicate with each other about the substance of the attorney-led litigation.

Target's attorneys also stayed involved nearly every step of the way. Internally, the Data Breach Task Force was co-chaired by Target's Chief Legal Officer and included several attorneys. Externally, Target's law firms retained Privileged Verizon and were parties to Privileged Verizon's engagement letter.

Not surprisingly, the only communications for which the court *did* compel productions were those that were not part of the separate investigation and did not include legal advice: Target was ordered to unredact various updates from Target's CEO to its board of directors.

Overall, Target's two-track investigation should be instructive to companies and their counsel who are still developing practices for dealing with a data breach. Defined workstreams and ongoing input from attorneys improve the odds of maintaining a claim of privilege over post-breach investigations on behalf of counsel.

Categories

Cybersecurity, Privacy & Data Protection

other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.