BRACEWELL

INSIGHTS

Privilege Dwindles for Data Breach Reports

August 9, 2021

By: ***Seth D. DuCharme***

Data privacy lawyers and cyber security incident response professionals are losing sleep over the growing number of federal courts ordering disclosure of post-data breach forensic reports. Following the decisions in ***Capital One*** and ***Clark Hill***, another district court has recently ***ordered*** the defendant in a data breach litigation to turn over the forensic report it believed was protected under the attorney-client privilege and work product doctrines. These three decisions help underscore that maintaining privilege over forensic reports may come down to the thinnest of margins—something organizations should keep in mind given the ever increasing risk of litigation that can follow a cybersecurity incident.

In May 2019, convenience store and gas station chain Rutter's received two alerts signaling a possible breach of their internal systems. The same day, Rutter's hired outside counsel to advise on potential breach notification obligations. Outside counsel immediately hired a forensic investigator to perform an analysis to determine the character and scope of the incident. Once litigation ensued, Rutter's withheld the forensic report from production on the basis of the attorney-client privilege and work product doctrines. Rutter's argued that both itself and outside counsel understood the report to be privileged because it was made in anticipation for litigation. The Court rejected this notion.

With respect to the work product doctrine, the Court stated that the doctrine only applies where identifiable or impending litigation is the "primary motivating purpose" of creating the document. The Court found that the forensic report in this case was not prepared for the prospect of litigation. The Court relied on the forensic investigator's statement of work which stated that the purpose of the investigation was to "determine whether unauthorized activity . . . resulted in the compromise of sensitive data." The Court decided that because Rutter's did not know whether a breach had even occurred when the forensic investigator was engaged, it could not have unilaterally believed that litigation would result.

The Court was also unpersuaded by the attorney-client privilege argument. Because the forensic report only discussed facts and did not involve "opinions and tactics," the Court held that the report and related communications were not protected by the attorney-client privilege. The Court emphasized that the attorney-client privilege does not protect communications of fact, nor communications merely because a legal issue can be identified.

The *Rutter's* decision comes on the heels of the *Capital One* and *Clark Hill* rulings, which both held that the defendants failed to show that the forensic reports were prepared solely in anticipation of litigation. In *Capital One*, the company hired outside counsel to manage the

cybersecurity vendor's investigation after the breach, however, the company already had a longstanding relationship and pre-existing agreement with the vendor. The Court found that the vendor's services and the terms of its new agreement were essentially the same both before and after the outside counsel's involvement. The Court also relied the fact that the forensic report was eventually shared with Capital One's internal response team, demonstrating that the report was created for various business purposes.

In response to the data breach in the *Clark Hill* case, the company hired a vendor to investigate and remediate the systems after the attack. The company also hired outside counsel, who in turn hired a second cybersecurity vendor to assist with litigation stemming from the attack. During the litigation, the company refused to turn over the forensic report prepared by the outside counsel's vendor. The Court rejected this "two-track" approach finding that the outside counsel's vendor report has not been prepared exclusively for use in preparation for litigation. Like in *Capital One*, the Court found, among other things, that the forensic report was shared not only with inside and outside counsel, but also with employees inside the company, IT, and the FBI.

As these cases demonstrate, the legal landscape around responding to security incidents has become filled with traps for the unwary. A coordinated response led by outside counsel is key to mitigating a data breach and ensuring the lines are not blurred between "ordinary course of business" factual reports and incident reports that are prepared for litigation purposes.