HINSHAW

Alerts

Capital One Loses Bid to Shield Post-Breach Report from Consumer Plaintiffs

June 29, 2020
Insights for Insurers: Cyber Coverage

On June 25, a Federal District Court in Virginia (Anthony J. Trenga, U.S.D.J.) affirmed a Magistrate Judge's Order requiring Capital One to produce a vendor's post-breach forensic report to plaintiffs in a consumer class action. In doing so, it rejected the bank's argument that the report was protected attorney work product.

Capital One had a forensic vendor, Mandiant, on a retainer to generally assist with cybersecurity matters, including any potential incident responses, prior to the 2019 data breach at issue. After the breach, Capital One and its outside counsel formally engaged Mandiant to conduct an investigation of the 2019 breach and prepare a written report. Capital One sought to have the Order set aside on various legal grounds, along with arguing the Order was "unworkable" and incentivized companies to (1) forego keeping an incident response vendor on retainer, or (2) hire a new, unfamiliar vendor to investigate incidents that are expected to result in litigation.

To set the Order aside, the district court said Capital One was required to prove that the post-breach report (1) was created when the litigation was a real likelihood and not when it was a mere possibility; and (2) would not have been created in essentially the same form in the absence of the litigation. Because there was no dispute concerning the first prong of the test, the court's analysis focused on the second prong, also known as the "but for" or "driving force" test. Capital One was required to demonstrate that the report would not have been prepared in substantially similar form *but for* the prospect of litigation.

Capital One asserted that Mandiant changed the nature of its investigation, the scope of work, and its purpose in anticipation of litigation. The bank further contended that Mandiant's investigation and report would have been very different if Mandiant had been engaged to investigate the breach for *business* purposes; a report prepared for business purposes would have focused on remediation, while a report prepared at the direction of counsel would focus on causation issues, according to Capital One.

That contention, the court stated, appeared "hollow" in light of the "identical" services covered under Mandiant's pre-breach agreement with Capital One and its post-breach engagement letter. The court said the primary difference between those two documents concerned the role that Capital One's outside counsel would play, and that Capital One failed to prove that the report would have been substantively different if it had been produced in the ordinary course of business absent the involvement of outside counsel.

The court also rejected Capital One's assertion that the Magistrate Judge should not have relied on the distribution of the post-breach report to approximately 50 employees, Capital One's board of directors, and regulators when deciding that the report was not entitled to work product protection, stating that "post-production disclosures are appropriately probative of the purposes for which the work product was initially produced."

The court then noted that Capital One's argument that the Order was unworkable "ignores the alternatives available to produce and protect work product, either through different vendors, different scopes of work and/or different investigation teams."

Related Content

In our prior post on this case, we discuss practical steps companies can take to protect post-breach reports from disclosure in light of the Capital One decision.