HINSHAW

Alerts

No Protection for Vendor's Forensic Report in Post-Breach Litigation?

June 16, 2020
Insights for Insurers

A May 26, 2020 order by U.S. Magistrate Judge John F. Anderson (E.D. Va.) that attorney work product protection did **not** preclude production of a forensic vendor's data breach investigation report to plaintiffs in the *Capital One* multidistrict litigation has rightly generated considerable buzz. While we await the outcome of Capital One's pending motion to set aside the order, we think the *Capital One* decision provides useful guidance about steps companies can take to protect forensic reports from disclosure in post-breach litigation.

Background

In 2015, Capital One executed a Master Services Agreement (MSA) with FireEye, Inc., d/b/a Mandiant to provide cybersecurity consulting services. The MSA was periodically supplemented with Statements of Work (SOW) for Mandiant to provide specified services, including incident response services, which were classified as "business critical." Following discovery of a massive data breach in March 2019, Capital One immediately retained outside counsel to provide legal advice concerning the incident. Several days later, outside counsel, Capital One, and Mandiant entered into a Letter Agreement pursuant to which Mandiant would provide incident response, digital forensic, and remediation services concerning the data breach at issue under the terms of its January 2019 SOW with Capital One. The Letter Agreement also provided that Mandiant's work would be done at the direction of counsel and that Mandiant's deliverables would be provided to counsel instead of Capital One. Plaintiffs began filing law suits against Capital One just one day after Capital One's July 2019 public announcement of the data breach.

On September 4, 2019, Mandiant issued its Report to outside counsel "detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security." Counsel subsequently provided the Report to Capital One's "legal department" and board of directors. The Report was also disclosed to approximately 50 Capital One employees, various regulators, and Capital One's outside accounting firm.

In the post-breach litigation, Capital One asserted the work product doctrine to prevent disclosure of the Mandiant report to plaintiffs. While noting that there was "no question" that Mandiant began its incident response services in July 2019, Magistrate Judge Anderson found that "the determinative issue concerning the work product protection issue was whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of that litigation." Magistrate Judge Anderson ruled that Capital One had the burden to show how it would have investigated the incident differently if there was no potential for litigation. He found that the fact that Mandiant prepared its Report at the direction of counsel did not satisfy the "but for" formulation.

In deciding that the Mandiant Report was not entitled to work product protection, the court highlighted various facts, including the following:

- Capital One and Mandiant had a pre-existing "paid retainer" under which Mandiant agreed to perform 285 hours of "essentially the same services" that were at issue in the motion to compel;
- Capital One had a long-standing relationship with Mandiant;
- As a financial institution, it was "critical" for Capital One to be in position to immediately respond to any potential compromise of the security of its systems;

- Capital One considered Mandiant's retainer to be a "business-critical expense" and not a legal expense at the time it was paid;
- The Mandiant report was distributed widely, including to (i) "fifty Capital One employees", (ii) four regulators (Federal Deposit Insurance Corporation, Federal Reserve Board, Consumer Financial Protection Bureau, and Office of the Comptroller of the Currency), and (iii) an accounting firm (Ernst & Young). Capital One offered "no explanation" as to why each recipient was provided with a copy of the Mandiant Report and whether the disclosure was related to a business purpose or for the purposes of litigation; and
- The disclosure of the Report to regulators and to Ernst & Young demonstrated that the results of the investigation were significant for regulatory and business reasons.

Guidance from the Decision

We do not believe that the *Capital One* decision should be treated as the death knell for protecting forensic reports from disclosure in post-breach litigation. Companies should, however, take into account the facts and outcome of this decision when deciding whether and how to engage with post-breach service providers. Companies that have existing relationships with cybersecurity vendors should consider (i) careful development of separate and incident-specific documentation to engage the vendor through outside counsel for the data breach at issue, or (ii) engagement of a new vendor through outside counsel if and when any data breach occurs. Companies also should thoughtfully consider whether a written report should be prepared by the vendor, and if so, carefully decide in advance how much detail should be included, how and to whom the report will be disclosed, and the reasons for any such disclosure in light of attorney-client privilege/work product protection concerns and the risk of discovery in litigation.