5 Takeaways From Capital One Breach Report Dispute

By **Colin Jennings, Ericka Johnson and Dylan Yépez** (June 23, 2020)

Colin Jennings

Ericka Johnson

Dylan Yépez

As has been widely reported, a magistrate judge in the U.S. District Court for the Eastern District of Virginia recently ordered Capital One Financial Corp. to produce a forensic report prepared by the cybersecurity firm Mandiant Inc., holding that the report was not protected as attorney work product despite having been prepared at the direction of outside counsel.

On June 9, Capital One filed an objection to that order, arguing that the magistrate judge misapplied the controlling law and improperly relied on Capital One's dual use of the Mandiant report for business-related purposes.

While the dispute regarding the discoverability of this forensic report continues, it is a good time to step back and on focus on the critical steps companies must take to protect privilege at the outset of a breach response.

Why is a privileged forensic report important?

A forensic report is normally prepared by a cybersecurity firm following a thorough investigation into the nature and scope of a company's cyberattack.

The report will generally detail, among other things, the critical vulnerabilities in a company's information technology environment that enabled the cyberattack, often identifying areas in which a company's IT defenses were not compliant with best practices, regulations and/or industry standards.

While these findings can help a company anticipate and defend against potential causes of action and mitigate risk, plaintiffs can also use this information as evidence to substantiate their claims. Therefore, plaintiffs, like those in Capital One, will seek to discover the report, while defendant companies will argue it is protected under the attorney work product doctrine.

What are the practical considerations going forward?

In determining whether a forensic report is privileged, courts will look to the totality of the circumstances. While Capital One's objection disputes the court's legal and factual reasoning, this debate provides a few practical takeaways to help make abundantly clear that a forensic report was created in anticipation of litigation.

1. Ensure that your outside counsel retains a cybersecurity vendor with which you have no preexisting relationship.

A company should, if possible, ensure that its outside counsel engages a forensic firm with which the company has no preexisting relationship for incident response services. Like Capital One, many companies enter into master service agreements and statements of work with forensic firms to receive incident response services prior to a cyberattack, as part of

their cyberrisk mitigation strategies.

Indeed, Capital One noted that "one purpose of the MSA and associated SOWs was to ensure that Capital One could quickly respond to a cybersecurity incident should one occur."

To obtain attorney work product protection, a company has the burden of proving that a forensic firm's work product was prepared in anticipation of litigation. However, the ruling in Capital One suggests that, to truly anticipate litigation, the scope of the forensic services must be determined after a cyberattack.

The Capital One court found it significant that Capital One failed to "show[] that Mandiant's scope of work under the Letter Agreement with outside counsel was any different than the scope of work for incident response services set forth in the existing SOW," or "that the nature of the work Mandiant had agreed to perform changed when outside counsel was retained."

Indeed, the court emphasized, "the statement of works and master services agreements provided for virtually identical services to be performed before and after the data breaches were discovered."

In response, Capital One argues that the relevant issue is not "the nature of the work Mandiant could have done for Capital One under the pre-existing SOW," but rather "the Report actually prepared by Mandiant under [outside counsel]'s direction."

Here, the preexisting SOW "broadly outline[d] the general types of incident response services that might be needed," leaving "the particular services" to be "determined on a case-by-case basis."

Further, Capital One asserts that the services underlying the Mandiant report were different from the services provided under preexisting SOWs for several reasons. First, Capital One retained outside counsel to help the company prepare for anticipated litigation, who in turn hired Mandiant to draft the report specifically "to inform and facilitate [outside counsel]'s investigation and advice."

And unlike the work underlying the report, "Mandiant did not do any incident response work for Capital One" for two years before the breach. Finally, Capital One conducted separate "internal business investigations parallel to [the] protected investigations," further distinguishing Mandiant's "protected, legal work [from] Capital One's ordinary-course, business investigation."

As we await the district court's ruling, the magistrate's order indicates that it may be prudent for companies to avoid engaging the same IT firm for litigation-related investigations as they rely on for business-related services.

2. Consider preemptively retaining a second cybersecurity firm for litigation-related investigations.

Following a data breach, it may be unfeasible to engage a cybersecurity firm with no preexisting relationship. As Capital One points out, under these circumstances, companies are "under the gun to determine whether there has in fact been an intrusion, the scope of the intrusion, and whether any sensitive data was exfiltrated."

Had Capital One's outside counsel used a vendor with which the company had no

relationship, "it would have taken weeks to months to approve a new vendor due to bank data security and regulatory obligations, as opposed to the hours or days a company has to effectively respond to a potential data breach."

To address these competing exigencies — i.e., clearing the regulatory hurdles of providing a new vendor access to sensitive information and systems, quickly responding to a cyberincident, and demonstrating that certain cybersecurity services are provided in anticipation of litigation — it may be prudent for counsel to engage a second forensic firm with which the company has no preexisting relationship.

This can provide a more thorough litigation and risk-mitigation focused review to supplement the incident response efforts and allow the company to demonstrate it has separate reports for business/regulatory and litigation purposes. By separating the businesses incident response from the prelitigation investigation, it is easier to demonstrate that the second forensic firm's analysis fits clearly within the work product protections.

3. Change your approach to vendors with a preexisting relationship.

Depending on the circumstances, neither of the above measures may be possible or desirable in connection with a breach event. If a company decides to use the same vendor for both business and litigation-related services, it is crucial to isolate the litigation-related services that the vendor provides and to detail them out in a separate SOW that makes clear how the scope and purpose of the litigation-related work differs from any preexisting SOWs.

The SOW should clarify, for example, that counsel is directing the work for the purpose of providing legal advice and guidance to the company in anticipation of litigation. And the SOW should not include any unrelated work such as remediation that may be covered under preexisting SOWs.

4. Use the report only for litigation purposes, and limit its disclosure to necessary individuals.

A company should use the forensic report solely for litigation purposes and should limit its distribution to only those who need it for these purposes. Such individuals may include in-house counsel, the board of directors and possibly a small group of cybersecurity employees who need to understand the full nature and scope of the attack and the vulnerabilities identified to assist counsel in the assessment of potential claims and defenses.

Clear direction needs to be provided to everyone that receives the report that it is privilege, confidential and not to be further disseminated. A company should not disclose a forensic report to third parties or the team responsible for incident response.

Generally, materials prepared in the ordinary course of business or pursuant to regulatory requirements are not documents prepared in anticipation of litigation.

In Capital One's case, the magistrate judge emphasized that about fifty employees, four regulators, an accounting firm, and the "corporate governance office general email box" received a copy of the forensic report. He stated:"[N]o explanation [was] provided as to why each recipient was provided with a copy" or "whether disclosure was related to a business purpose or for the purpose of litigation."

Further, "Capital One anticipated using the Mandiant Report in making certain disclosures

required under the Sarbanes Oxley Act" and provided the report to an employee "for 2nd line business need."

Capital One also "fail[ed] to address what, if any, restrictions were placed on those persons and entities who received a copy." In considering these factors, the court ultimately determined that Capital One used the report for various business and regulatory purposes.

In its recent objection, Capital One does not dispute that the Mandiant report was used for purposes beyond litigation, but maintains that such dual use does not destroy the work product protection:

Regardless of whether Capital One had other, business reasons to investigate the cyberincident, those reasons arose from the same set of facts that created the threat of litigation and occasioned Mandiant's investigation.

Similarly, Capital One argues that its disclosure of the report to a limited number of recipients is immaterial. It disclosed the report to governmental regulators because it is obligated to do so. It disclosed the report to its auditor, Ernst & Young LLP, and outside counsel directed Mandiant to communicate with Ernst & Young, "to confirm that the Cyber Incident did not impact the integrity of Capital One's internal controls over financial reporting."

It disclosed the report to a small number of employees on a need-to-know basis, and distribution was "'tightly controlled,' 'monitored,' and 'logg[ed]' by Capital One's Senior Associate General Counsel." And it used the report to make Sarbanes-Oxley disclosures for the "distinctly legal purpose" of "minimiz[ing] the risk of regulatory action and litigation."

No matter the final decision, the safest course of action is to provide the full report only to those who need it solely for litigation purposes and provide clear controls on its use. As a practical matter, companies can often create a separate and nonprivileged report to be used for business and regulatory purposes.

Nonprivileged reports should be distinct from the privileged forensic report, i.e., not a copy and paste job, and should provide a summary of their findings rather than a detailed analysis.

5. Pay for litigation-related cybersecurity services from your litigation or legal budget.

A company should pay for incident response services out of its litigation or legal budget to show that a forensic firm's services were provided in anticipation of litigation, as opposed to a business expense.

Capital One paid for Mandiant's services under the letter agreement from the preexisting SOW retainer until the retainer was exhausted and from its cyberorganization's budget thereafter. Capital One designated the fees as a business critical expense and not a legal expense.

After the cyberattack, Capital One reclassified the expenses associated with Mandiant's work on the data breach as legal expenses and deducted them from its legal department's budget.

The court was not persuaded, finding that "the retainer paid to Mandiant was considered a

business-critical expense and not a legal expense at the time it was paid." In considering this factor, the court ultimately determined that Capital One had requested the report for various business purposes.

In response, Capital One points out that the company had initially classified the retainers paid to Mandiant before the data breach as business critical expenses rather than legal expenses, because regulations require the company to have a plan in place for cybersecurity incident response.

Irrespective of how the court resolves this dispute, companies should pay close attention to how they pay and account for cybersecurity and incident response services to clearly differentiate business and legal functions.

When appropriate, retainers or similar payments should be allocated to a legal function and accounting entries should be written to demonstrate the legal purpose of the work to be undertaken.

In any event, before incurring the expenses, companies should consider designating the costs of incident response services to their legal budgets to show that such services are provided in anticipation of litigation.

Colin Jennings is a partner, and Ericka Johnson and Dylan Yépez are associates, at Squire Patton Boggs LLP.