JUNE 11, 2020

Data breach aftermath: Court orders disclosure of a forensic consulting firm's confidential report to class plaintiffs

By Tina Sciocchetti, Bruce Copeland, Jenny Holmes, Jason Gonzalez, and Alycia Ziarno

When a company suffers a data breach affecting its customers or employees, its first step is typically to seek the assistance of a forensic consulting firm that will investigate the cause of the breach, identify susceptibilities in the company's systems, and assist in remediation. Traditionally, forensic consulting firms are hired through legal counsel in anticipation of litigation, in order to protect the consulting firm's work product under the auspices of the attorney-client and work product legal privileges. Companies usually expect the results of these breach investigations to remain confidential and take steps to mitigate against disclosure. But, a recent decision highlights the growing risk that the findings of forensic consulting firms, along with their identification of potential weaknesses in a company's systems and security failures, may no longer be only for the eyes of the company executives and counsel who procure them.

A Virginia federal court has compelled the production of a forensic consulting firm's report in a consumer class action stemming from a 2019 data breach at Capital One. At issue in the case was whether the consultant's report constituted protected "work product" prepared in anticipation of litigation. Following discovery of the breach, the company had immediately engaged outside legal counsel, which in turn quickly executed a "letter agreement" (along with Capital One) with a forensic consulting firm that had already been on retainer with the company, to provide "services and advice" related to the breach. Under the letter agreement, the consultant was to work at the direction of, and report to, outside counsel. Within days, the company publicly announced the breach, and litigation ensued immediately. Thereafter, the consulting firm prepared a report of its investigation for counsel, including details about the technical factors that allowed the hacker penetration of Capital One's systems. Plaintiffs sought the consultant's report in discovery, and Capital One objected to disclosure, citing work product protections.

Despite the context and timing of the forensic consultant's work on behalf of Capital One in relation to the breach litigation, the court ordered disclosure of the consultant's report to plaintiffs in the case, holding that it did not constitute protected work product. Stating that assertions of evidentiary privileges such as work product are disfavored because "they shield evidence from the truth-seeking process," and are "narrowly and strictly construed," the court ruled Capital One had

failed to establish that it would not have commissioned the report "but for" the threat of litigation following the breach. That is, the company failed to demonstrate "that the incident response services [the consultant] performed would not have been done in substantially similar form even if there was no prospect of litigation."

In concluding that the consultant's report was not prepared in anticipation of litigation, the court relied on three principal factors: (i) the preexistence of a master services agreement (MSA) between Capital One and the consultant, the terms of which were incorporated into the letter agreement with legal counsel; (ii) the manner in which the consultant was paid for its services; and (iii) the prior, unexplained disclosure of the forensic report to multiple individuals.

Existing master services agreement

Critical to the court's decision was the timeline reflecting the consultant's ongoing relationship with Capital One. The company entered into the MSA with the consultant nearly four years before the breach at issue, in November 2015. Thereafter, the company issued periodic statements of work (SOWs) and purchase orders under the MSA. The court observed the purpose of the MSA and SOWs were to allow Capital One to immediately respond to any potential compromise of the security of its systems by providing for incident response services in the event such services were necessary. Further, the company categorized the retainer paid to the forensic consultant as a business—rather than a legal—expense.

Shortly before the March 2019 data breach, Capital One had executed an additional SOW and paid a retainer allowing for 285 hours of services. Capital One confirmed the subject breach in July, and retained counsel the following day. Within days, along with counsel, it executed the letter agreement that governed the services and advice the consultant provided in connection with the data breach. As noted, the letter specified the work was to be done at the direction of counsel and that deliverables would be provided to counsel instead of Capital One.

According to the court, to avoid disclosure of the report to plaintiffs in discovery, Capital One bore the burden of "showing how it would have investigated the incident differently if there was no potential for litigation." The hiring of outside counsel who directed the consultant's work was not dispositive because the company still had to "conduct[] its duties and address[] the issues at hand" following the breach. The court pointed to the long-standing MSA with the consultant and the existing SOW "to perform essentially the same services that were performed in preparing the subject report," and found no evidence that the company would not have called upon the consultant to conduct the very same services and issue the same report in the absence of litigation.

Although the consultant was not performing an ongoing investigation at the time of the subject data breach when it entered into the letter agreement to perform work, the court found the existing SOW with a paid retainer significant. The letter agreement did not change the terms of the SOW or the type of work for incident response services the consultant was already engaged to perform, even if the work was to be directed by legal counsel and the report delivered to counsel in the first instance. The company failed to show that "*the nature of the work*" the consultant had agreed to perform was changed when outside legal counsel was retained. Rather, the existing MSA and SOW were "effectively transferred to outside counsel" and "the retention of outside counsel [did] not, by itself, turn a document into work product."

Payment of fees

In addition to the existing SOW, the court noted that the consultant was paid from the previously existing retainer. The court further emphasized the fact that the retainer was from the business expense budget and not a legal expense demonstrated that this was not prepared "but for" the threat of litigation.

Prior disclosure of report

Also affecting the outcome of the court's ruling was the fact that the consultant's report had been shared with multiple individuals outside of legal counsel. Following submission of the report to counsel, it was shared with the company's legal department, its board of directors, and approximately fifty employees, as well as four external regulators and an accounting firm. The court found no explanation for the disclosures and whether each served a business, regulatory, or litigation purpose. Capital One was further faulted by the court for failing to address whether any recipient had been advised of restrictions on discussing, copying, or disseminating the report or any portions of it to others. The court noted the company had also planned to use the report in connection with disclosures required by Sarbanes Oxley Act, and it had been referenced in materials prepared for the company's public disclosure of the breach.

The court distinguished a prior decision with substantially similar facts that had oppositely ruled the forensic consultant's report of a data breach was protected work product on the basis that in the prior case, the report had not been provided to the company's incident response team, whereas here, several Capital One employees had been given the report and it was used for business and regulatory purposes. While the court reasoned that the distribution of the report to others did not necessarily constitute "a waiver" of the privilege, "it [did] show that the results of an independent investigation into the cause and the extent of the data breach was significant for business and regulatory reasons" outside of the threat of pending litigation.

Takeaways

Although the Capital One decision illustrates circumstances in which a company might risk disclosure of a confidential forensic data breach report to opposing litigants, the decision is also instructive of steps that can be taken to protect the privileged nature of such reports. Whether or not a company has an ongoing contractual relationship with a forensic consulting firm at the time of a data breach, consider the following:

Consult with counsel

Before engaging a consulting firm to handle the response to a data breach incident, discuss your options with counsel. In consultation with counsel, you can determine whether to engage an existing consultant (who may have detected the breach and already be familiar with your company's systems) to perform an investigation or to retain a separate consultant in anticipation of litigation related to the new data breach). Counsel can advise the nature of the engagement and help decide whether you plan to disclose the resulting report in any subsequent litigation, or instead wish to take steps to protect the report as non-discoverable work product. To increase the probability that a court will treat the resulting consultant's report as work product, counsel should engage the forensic consultant and direct its work, under terms separate and distinct from any ongoing services agreements with the consultant.

Separate prior engagements

If a company has an ongoing relationship with a consulting firm and wishes to utilize the same consultant for the incident response at hand, it is imperative that the engagement and scope of work remain separate from any ongoing relationship. The nature and scope of work should be distinct from generalized ongoing services and customized to the extent possible to the current data breach. If the scope of work cannot be sufficiently distinguished from a consultant's ongoing obligations, it may be advisable to retain a separate firm for the breach investigation to enhance the work product nature of the resulting report. Keep in mind that an existing consultant familiar with your systems, and prior breach history or possible vulnerabilities, can advise another consultant to create efficiencies and lower costs.

Separate fees

The engagement of a forensic consultant for services related to a data breach should include payments and invoices separate from any existing agreements with that consultant.

Limit distribution

While the distribution of a consultant's report to individuals outside of independent legal counsel does not necessarily constitute a waiver of privilege, it is important to give careful thought to the purposes for such disclosure and whether every disclosure is necessary. Increasing the "business" and "regulatory" purposes to which a report is applied, as opposed to "legal" or "litigation-related," increases the risk that it will be viewed as non-work product. Limited distribution can demonstrate the confidential and protected manner in which the report was handled, as can specific instructions to recipients about the manner in which the report is to be utilized, copied, and further distributed (if at all).

Plan for the possibility of disclosure

As the Capital One case demonstrates, even the best-laid plans may not protect the confidential and protected nature of a consultant's data breach report. Together with counsel, plan for appropriate content and form of the consultant's report with the expectation that the report may be ordered disclosed in ensuing litigation. If a protective order is not in place in litigation, be certain to obtain a protective order from the court before any disclosure of the consultant's report is made.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

- Tina Sciocchetti, 518-427-2677, **tsciocchetti@nixonpeabody.com**
- Bruce Copeland, 415-984-8253, **bcopeland@nixonpeabody.com**
- Jenny Holmes, 585-263-1494, **jholmes@nixonpeabody.com**
- Jason Gonzalez, 213-629-6019, **jgonzalez@nixonpeabody.com**
- Alycia Ziarno, 202-585-8265, **aziarno@nixonpeabody.com**