Insights: Alerts

Recent Court Decision Carries Lessons for Retaining and Using Cybersecurity Consultants to Investigate a Breach

July 17, 2020

Written by **Anthony D. Glosson, Clay C. Wheeler** and **Jon Neiditz**

A recent federal district court decision underscores the importance of structuring breach investigations with the attorney work-product doctrine in mind. In *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 3470261 (E.D. Va. June 25, 2020), the U.S. District Court for Eastern District of Virginia upheld the magistrate judge's recommendation that a breach report compiled by a cybersecurity firm was not protected work product, even though the firm had reported to Capital One's outside counsel during the investigation. *Id.* at *7.

In *Capital One*, the bank hired the cybersecurity firm prior to any breach. The companies signed a master services agreement ("MSA") and multiple statements of work ("SOW"), including a January 2019 SOW which included breach response and remediation services. Half-a-year later, Capital One uncovered a data breach and hired outside counsel shortly thereafter. Outside counsel and the cybersecurity firm executed a letter agreement, which included a scope-of-work description copied verbatim from the January 2019 SOW and required the cybersecurity firm to complete the work in accordance with the specifications and payment terms set forth in that earlier SOW and the underlying MSA. The letter specified, however, that the cybersecurity firm was working under the direction of counsel.

The cybersecurity firm originally only sent the breach report to outside counsel, but eventually circulated it to Capital One's Board of Directors, outside auditor, employees, and financial regulators. The court ruled that Capital One could not show that the breach report's main purpose was for litigation purposes rather than for a business need: "it would be unreasonable to think, given identical contractual obligations under the pre- and post-data breach SOWs, that had [the cybersecurity firm] not provided to Capital One through [outside counsel] all the information required under the SOW concerning the breach, it would not have provided that same 'business critical' information directly to Capital One in discharge of its obligations under the pre-data breach MSA and SOW." *Id*. at 6. Capital One's broad sharing of the report underscored Capital One's "business needs" for the report. *Id.*

The decision could reverse the positive trend of companies proactively engaging security consultants to manage future breaches. Indeed, some commentators have suggested retaining a different cybersecurity firm to do breach remediation, rather than continuing with the same firm used for general cybersecurity advice, in order to differentiate the unique, legal purpose behind the resulting report. However, such dramatic action may not

always be necessary. Here are 4 specific takeaways for companies that are reasonably concerned about the decision and the prospect of disclosing a breach report to opposing counsel:

1. **Involve counsel in all aspects of the breach investigation.** The good news is that the *Capital One* decision need not put a damper on proactive cybersecurity hygiene. Instead, it serves to underscore the importance of involving counsel in a substantive way in breach prevention, response, and remediation. The critical issue that the court had with the Capital One breach report was that the report's purpose was overwhelmingly business-related, rather than in anticipation of litigation. If outside counsel is heavily involved in the breach investigation and report drafting, counsel can structure the report so that it in fact helps to prepare for litigation. Such involvement will help ensure that a breach report does not appear solely business-focused. Further, counsel's involvement may strengthen an argument for attorney-client privilege, so that a company is not restricted to claiming only work-product doctrine protection in order to protect the breach report.

2. **Do not shy away from using a preferred cybersecurity consultant for breach remediation.** While retaining a new consultant may aid one's work-product doctrine argument, it risks producing an inferior and inefficient outcome because the new consultant will face a steep learning curve in familiarizing itself with a company's business practices, network configuration, application portfolio, and overall cybersecurity posture, all while time is of the essence. By contrast, a company's existing consultant will have a built-in advantage by understanding these company-specific dynamics. In most cases, the existing consultant will be better equipped to deliver competent analysis and remediation. As stated above, the key question for a court is whether the report is created primarily for business reasons or if the report has a critical litigation purpose; counsel's substantive involvement in the breach investigation and report drafting will help safeguard a report's protection.

3. **Retain security consultants who understand the law and legal counsel who understand cybersecurity.** Although companies may still use their preferred cybersecurity consultants for breach remediation, they generally seek cybersecurity consultants who demonstrate familiarity with the concepts of attorney-client privilege and work-product doctrine under the applicable law and are used to working with counsel. Correspondingly, outside counsel must understand the intricacies of the cybersecurity field, including evidence gathering, and have experience working with consultants hired by a client. While hiring lawyers and cybersecurity consultants who “play well together” has always been desirable, the *Capital One* decision demonstrates the practical importance of that principle in protecting sensitive documents during discovery.

4. **Consider preparing two different reports following a breach.** While there may be sound business reasons to broadly share a breach report, as Capital One did, companies may want to consider having their outside counsel and cybersecurity consultants prepare two different breach reports: (1) a detailed, litigation-focused report intended to be circulated within the legal department and C-suite on a need-to-know basis and in anticipation of litigation, and (2) a second report at a higher level of detail and analysis, that can be circulated more broadly, but may ultimately be produced be in discovery.

Kilpatrick Townsend & Stockton LLP has extensive experience structuring consultant relationships to align with best practices, deep technical knowledge enabling us to coordinate closely with cybersecurity experts at every step in breach prevention, detection, and remediation, and practical expertise in conducting complex internal investigations. When litigation is a real possibility, these skill sets are indispensable assets in protecting some of the most sensitive confidential information that a company collects in a time of crisis: the details of its cybersecurity posture before and after an incident occurs.

Related People

Anthony D. Glosson

t 202.508.5842

tglosson@ktslaw.com

Clay C. Wheeler

t 919.420.1717

cwheeler@ktslaw.com

Jon Neiditz

t 404.815.6004

jneiditz@ktslaw.com