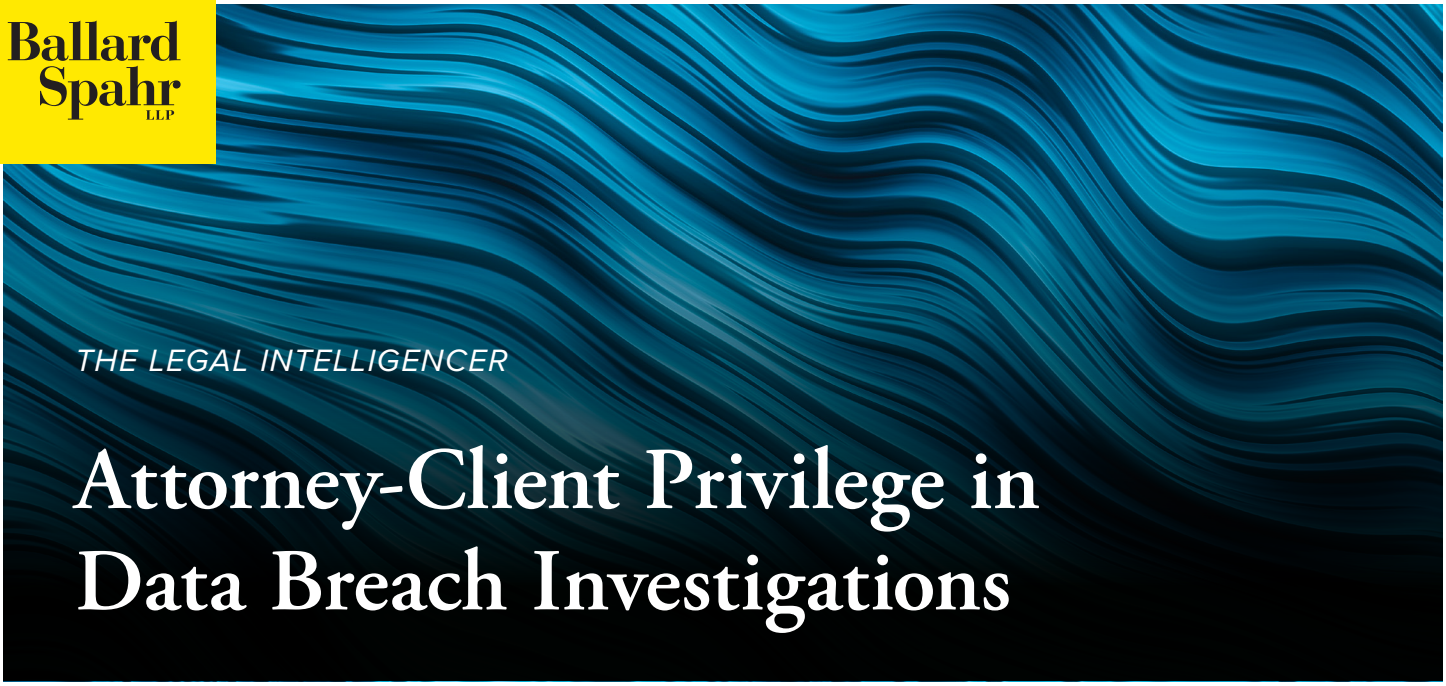
Ballard Spahr LLP



THE LEGAL INTELLIGENCER

Attorney-Client Privilege in Data Breach Investigations

July 3, 2022

By Philip N. Yannella and Timothy W. Dickens

In recent years, several federal courts have rejected claims of attorney-client and work product privilege in connection with forensic analysis post-data breach. Whereas in the past, parties assumed that such reports would be protected from discovery in data breach lawsuits or regulatory investigations, recent decisions suggest that courts do not automatically assume that forensic experts are retained for legal purposes following a data breach, complicating companies' incident response processes.

There are, however, steps that companies and lawyers can take to bolster claims of privilege relating to forensic examinations. This article will analyze two recent cases to identify pitfalls and outline current trends used by companies and their lawyers to try to protect forensic findings and communications.

Recent Cases

As litigators know well, the work-product doctrine provides protection for materials prepared in anticipation of litigation or for trial. See Fed. R. Evid. 502(g)(2). The fact that there is litigation does not, alone, cloak materials with work product immunity. Instead, the materials must be prepared because of the prospect of litigation. Materials prepared in the ordinary course of business, pursuant to regulatory requirements, or for other nonlitigation purposes are not documents prepared in anticipation of litigation and therefore may be subject to discovery. Similarly, the attorney-client privilege protects communications made between privileged persons in confidence for the purpose of obtaining or providing legal assistance for the client. See *Teleglobe Communications,* 493 F.3d 345 (3d Cir. 2007). Privileged persons generally include the client, attorneys, and any of their agents that help facilitate the attorney-client communications or legal representation. Evidentiary privileges are generally disfavored because they shield evidence from the truth-seeking process. They are therefore construed narrowly and the party asserting the protection bears the burden of demonstrating applicability.

Beginning with *In re Capital One Consumer Data Security Breach Litigation,* No. 19-2915, 2020 U.S. Dist. Lexis 91736 (E.D. Va. May 26, 2020), the U.S. District Court for the Eastern District of Virginia rejected arguments that a forensic incident report commissioned through the defendant's outside counsel constituted protected work product.

The timeline and circumstances of this breach are relatively standard. Four years prior to the breach, Capital One entered into a master service agreement (MSA) with its vendor to provide broad remediation support in the event of a cybersecurity incident. The MSA called for the vendor to provide a detailed final technical report covering its activities, the results of its testing, and recommendations for recovery and remediation at the conclusion of the incident. Capital One paid for the vendor's services as a "business critical" rather than "legal" expense.

Once a breach was identified in July 2019, Capital One retained outside counsel to provide legal advice regarding the incident. Capital One's outside counsel signed a separate agreement with Capital One's existing vendor to investigate and remediate the breach. This agreement (the outside counsel agreement) stated that the payment terms "were to be the same as those" set out in the most recent MSA between Capital One and its vendor, and that the parties would "abide by the applicable terms" therein. The primary difference between the original MSA and the outside counsel agreement was that the latter provided for work to "be done at the direction of counsel" and for deliverables to be provided to counsel instead of Capital One.

Once the report was finalized, the vendor shared the report with Capital One's outside counsel, who shared the report with Capital One's legal team. In addition to the legal team, Capital One shared the report with its board of directors, 50 Capital One employees, four regulators and its accounting firm. Capital One did not provide legal grounds for sharing the report or provide information on restrictions limiting the use and disclosure of the report.

The district court in *Capital One* acknowledged that there was "no question" that there was a very real potential of litigation following the breach. Therefore, the court moved to the next prong—establishing that the report at issue was created "because of" litigation and would not have been created in a substantially similar format otherwise.

The court summarily rejected Capital One's claims that the report would not have been completed in substantially the same manner but for the prospect of litigation. First, the court found that the fact that the investigation was completed at the direction of—and initially provided to—outside counsel rather than Capital One was not sufficient to establish work product protection. Next, the Court highlighted that both the MSA and the relationship between the vendor and Capital One prior to the breach and following the breach were essentially identical. Further, the retainer was initially paid for as a business expense rather than a legal expense. These factors suggested that the report was in fact a business continuity product as much as—if not more than—a litigation product. The court also highlighted that the report was shared relatively broadly outside of Capital One's legal team and used for a wide variety of purposes, including continuity, regulatory reporting and accounting. Therefore, the court found that Capital One had failed to establish how the report generated under the outside counsel agreement would have been any different than a report generated for other purposes that would have been necessary even without the prospect of litigation.

Other courts have gone further, questioning whether communications generated in the course of a breach investigation are protected by the attorney client privilege. In *Wengui v. Clark Hill*, for example, a client sued his former law firm after a data breach resulted in public exposure of the client's protected data. Similar to Capital One, the firm's outside counsel employed a cybersecurity provider to investigate and remediate the breach. The vendor provided a report that included findings and detailed recommendations for tightening the firm's cybersecurity operations. The firm argued that the report was protected by the work product doctrine and attorney-client privilege.

The District of D.C. rejected arguments that the report could be protected under the attorney-client privilege. The court acknowledged the attorney-client privilege may extend to third party reports made at the request of the attorney or client, where the purpose was to facilitate the attorney client relationship. But, this exception must be construed narrowly. To that end, "if the advice sought by the client is the professional consultant's rather than the lawyer's, no privilege exists." Because the report contained "not only a summary of the firm's findings, but also pages of specific recommendations on how the firm should tighten its cybersecurity," and because it was used by the both the firm's IT team for remediation and the FBI for investigation, the court found that the report was obtained primarily for general

cybersecurity expertise rather than legal advice. Therefore, the court rejected defendant's arguments that the report could be protected under the attorney-client privilege. A similar result was reached in In re Rutter's Data Security Breach Litigation, 2021 U.S. Dist. LEXIS 136220 (M.D. Pa. May 26, 2020), where the court found that the defendant had failed to establish that the report involved presented legal opinions or tactics rather than mere facts regarding the incident, which are not subject to the attorney-client privilege.

Best Practices to Privilege Breach Investigations

Although these cases appear to weaken the availability of the attorney-client privilege and work product doctrine in the context of breach investigations, they are instructive for businesses seeking to protect incident reports.

First, businesses should consider using a dual track for breach investigations. This approach would clearly distinguish between a privileged litigation-focused investigation and a general business continuity investigation. These investigations should be conducted under separate contracts that clearly distinguish their scope and purposes. Similarly, a business that keeps a forensic vendor on retainer should clearly distinguish between pre- and post-breach services. By separating these investigations, businesses and outside counsel can avoid arguments that the breadth of any report created extend beyond the scope of litigation concerns.

Second, when contracting, businesses must pay for the vendor as a legal expense. While paying for the vendor as a legal expense alone is unlikely to result in a finding of work product or privilege, it avoids the argument that the business viewed the report as a business continuity rather than legal product.

Finally, businesses should ensure that any report intended to remain privileged is not disseminated outside of the businesses' legal team and outside counsel. Any dissemination within the legal team should be subject to explicit controls to ensure that only non-legal members who are needed to implement legal strategy receive the report. Further, the report should not be shared for purposes of regulatory compliance, which may be seen as a nonlitigation purpose. Instead, where necessary, businesses should have information separately summarized in a manner that limits the information disclosed and ensures the confidentiality of the original report. Alternatively, where possible, businesses should consider releasing information to regulators from a no-privileged business continuity report.

As the rate of cyber incidents and litigation continue to rise, businesses and counsel need to stay abreast of developments privilege and work product precedent. By establishing and maintaining clear breach response plans prior to an incident, businesses will be better positioned to respond to incidents in a manner that ensures business continuity and limits liability.

Philip N. Yannella *is practice co-leader of Ballard Spahr's privacy and data security group, and practice leader of the firm's e-discovery and data management group. Timothy W. Dickens is an associate in the privacy and data security group.*