GT GreenbergTraurig

Alert | Data Privacy & Cybersecurity

February 2025

Privilege Under Pressure: The Shifting Data Breach Investigation Landscape

Go-To Guide

- Recent case law shows skepticism by some courts when evaluating whether forensic reports prepared after a data breach are protected under privilege, with some courts questioning privilege over communications with the client and counsel where the forensic firm is copied.
- Companies may consider reviewing their practices for managing breach investigation communications and information sharing.
- To preserve confidentiality, companies should consider managing who receives breach investigation updates and how they are delivered.

Over the past few years, the rate of notable data breaches has risen considerably, and along with that rise has come an increase in class action litigation. In a world where any company can be the next victim of a breach, business leaders and their legal counsel should consider in advance how to protect privilege and minimize risk in post-breach investigations. But certain recent federal district court decisions have made it more difficult to assert protection over breach-related documents and communications.

Traditional Approach to Data Breaches: Forensic Reports

Traditionally, after data breaches of all sizes, outside counsel's standard approach has been to hire highly technical vendors, such as forensic investigators, to perform the analysis of how a breach unfolded to inform their legal advice. This approach creates a three-way relationship focused on providing companies with the best legal advice possible after a breach. The forensic firm's role in such situations is as a consulting expert, often providing a comprehensive report to support legal counsel's efforts. Previously, lawsuits after a breach were rare, and challenges to defendants' breach investigation methods were even more uncommon. Thus, collaboration between companies' legal counsel and forensic firms proceeded unquestioned.

The CCPA's Potential Effect on the Landscape

Since 2020, the number of lawsuits filed after data breaches have increased dramatically, especially where a significant number of individuals' personal information is exposed. The reason for the increase may be California's data privacy law, the CCPA[1], which allows plaintiffs to claim statutory damages of $100 to $750 per affected person. While damages are limited to California residents, plaintiffs' lawyers have persisted in filing nationwide class actions involving non-Californians, resulting in a proliferation of lawsuits. These lawsuits have led to increasing challenges against keeping forensic reports protected under privilege.

Forensic Reports and Discovery

During the discovery phase of a lawsuit, lawyers are entitled to request relevant documents and communications from the opposing party. For forensic reports, counsel typically claims at least one type of protection, whether via the work product doctrine, attorney-client privilege, or both. Work product protection is permitted when a document was created "in anticipation of litigation," either by counsel or by a non-lawyer at counsel's direction.[2] As seen in case law, the facts of how and why a document was created determine whether its purpose was primarily for litigation or merely business purposes.

Attorney-client privilege generally applies to (1) a communication; (2) made between privileged persons; (3) in confidence; (4) for the purpose of seeking, obtaining, or providing legal assistance to the client.[3] While powerful, it can be waived, such as by sharing communications with certain third parties. And it does not protect underlying facts, though the communications themselves often contain a mix of facts and opinions.

But recent cases—discussed below—show that findings of protection over forensic reports are by no means assured. On top of courts' new tendency to find that there is no guarantee of protection when counsel directly retains a forensic investigator in certain circumstances, a recent federal district court case has also excluded from protection communications between the victim company, counsel, and the forensic investigator.

Federal Courts Narrow the Scope of Protection

In the last few years, certain federal district courts across the nation have begun issuing decisions slimming the scope of protection for forensic reports produced in response to a data breach. An early

[1] California Consumer Privacy Act (CCPA), Cal. Civ. Code § 1798.150 (a)(1) (2018). The threshold for such lawsuits is low, requiring a showing that the breached entity failed to have reasonable security.
[2] Fed. R. Civ. P. 26(b)(3).
[3] *Wengui v. Clark Hill PLC*, No. 19-3195 (D.D.C. Jan. 12, 2021).

notable case was *Capital One*[4] in 2020, which found no work product protection attached to the forensic report. The dispute over work product protection arose in large part because the forensic investigator was on retainer with the victim company before the breach occurred, even though the investigator conducted its investigation pursuant to a separate statement of work that outside counsel requested. The court held that even though litigation may have been likely when the report was made, the report was ultimately prepared for business purposes because the facts proved a similar report would have been created anyway. Capital One did not appeal this ruling.

In 2021, *Wengui* held that there was no work product protection when a separate forensic firm drafted a forensic report at counsel's request, despite the report being created in parallel to a report the defendant corporation's IT security advisor prepared, because the forensic report was still used for business purposes. The court also held that attorney-client privilege did not apply to this report because the facts showed the defendant corporation was seeking the investigator's technical advice directly, rather than relying solely on their attorney's legal advice as aided by the investigator's findings.

Several months later, *Rutter's*[5] found work product protection only applies where "'identifiable' or 'impending' litigation is the 'primary motivating purpose'" of creating the document. Because the defendant suspected, but did not know for sure, whether a breach had occurred at the time it engaged the forensic investigator, the court decided the defendant could not have "unilaterally believed that litigation *would* result."

As to the attorney-client privilege, the *Rutter's* court found it does not exist where the forensic report only discusses facts and does not involve "opinions and tactics," noting that the privilege does not protect any communications of fact, nor does it apply merely because a legal issue is present.

An opinion from the Western District of Washington, *Leonard v. McMenamins*,[6] continues this recent trend, but with a twist – the plaintiff requested both the forensic report and counsel's email communications to the client where the forensic firm was copied. In *Leonard*, the defendant corporation suffered a ransomware attack. External counsel hired a forensic investigator, which investigated at counsel's direction and prepared a forensic report. The defendant claimed both work product and attorney client privilege over the report. The court disagreed on both fronts.

For the report, the court found work product protection was not present, relying on prior persuasive cases to develop a list of factors: (1) whether the report provides factual information to the breached company; (2) whether the report is the only analysis of the breach; (3) the kinds of services the retained investigator provided; (4) the relationship between the retained investigator and the breached company; and (5) "whether the report would have been prepared in a substantially similar form absent the anticipation of litigation."

Ultimately, the court based its opinion on its finding that the report was drafted for a purely business purpose. Because the report was, in the court's view, the only source of meaningful analysis about the breach, it held the plaintiffs would have met the Rule 26(b)[7] exception to work product privilege. That exception permits a party to overcome a work product privilege claim by demonstrating that documents are (1) otherwise discoverable under Rule 26(b), and (2) the party can show it has "substantial need" for

[4] *In re. Capital One Consumer Data Security Breach Litig.*, No. 1:19md2915 (AJT/JFA) (May 26, 2020).
[5] *In re. Rutter's Inc. Data Security Breach Litig.*, No. 1:2020cv00382 (M.D. Penn. August 21, 2021).
[6] *Leonard v. McMenamins Inc.,* No. C22-0094-KKE (W. D. Wash. Dec. 6, 2023).
[7] Fed. R. Civ. P. 26(b)(3)(A) requires plaintiffs to demonstrate a "substantial need" and "undue hardship" if the document were barred from discovery.

the documents to support its arguments and would take on "undue hardship" if required to obtain similar documents by other means.

Regarding attorney-client privilege for the report, the court placed great weight on whether legal advice is sought when requesting the forensic report, but even greater weight on whether such advice is in fact provided. In the end, because the report in *Leonard* "does not provide legal advice," the court found it was not privileged.

Leonard is unique because the court addressed more than just materials the forensic investigator prepared; it evaluated counsel's emails to the client where the forensic firm was copied. After the defendant asserted attorney-client privilege, the court elucidated its view that "communications involving [the forensic investigator] concerning the facts of the attack and [the defendant's] response, investigation(s) and remediation are not privileged." The court did leave the door open for at least some email communications with counsel to remain privileged, noting that "[t]here can be circumstances when a cybersecurity consultant works with counsel to provide legal advice after a data breach." However, in a footnote, the court expressed its expectation that, in that case, "most, if not all, communications that include [the forensic investigator] will be removed from the privilege log and produced." The court may have been alluding to the *Kovel* doctrine, which provides that attorney-client privilege can attach to communications with third party consultants if their primary purpose is to give or receive legal advice, as opposed to business or tax advice.[8] The *Leonard* court did not acknowledge *Kovel* explicitly, relying primarily on tests that emphasize the nature of the privilege.[9]

Conclusion

While many courts have protected forensic reports and communications from disclosure in litigation, the emergence of this more restrictive view may require companies to exercise caution and restraint when communicating with forensic investigators. Recent cases have focused on whether a forensic firm is truly assisting legal counsel with providing advice, or instead performing the business function of analyzing how a breach occurred. When examining protection in light of the increasing likelihood a class action is filed after a significant breach, courts appear to be struggling to align on whether that risk is the true reason reports are prepared and whether the forensic investigator is truly providing expertise to aid legal counsel. At a time when litigation following a data breach is surging, lending credibility to the argument that forensic reports are prepared in anticipation of such litigation, courts are grappling with this essential question: what is the true role of a forensic investigator following a data breach?

Takeaways

When breaches occur, attorneys can react proactively to this district court trend. Companies may want to consider the following:

- Assume privilege will not apply to communications with a forensic firm.
- When possible, save substantive updates about the breach for phone calls where participants can be controlled and not emails, which can be easily forwarded, jeopardizing privilege.
- Ensure the engagement letter between counsel and the forensic investigator clearly sets forth the risk of litigation because of the breach and need for counsel to advise the victim company on its legal obligations and risks.

[8] *United States v. Kovel*, 296 F. 2d 918 (2d Cir. 1961).
[9] *See Leonard*, at *8.

- In breaches that may give rise to litigation risk (e.g., for companies processing significant amounts of sensitive personal data), consider whether issuing a litigation hold at the outset of the investigation is prudent.
- Review forensic reports live with the investigator and client to provide feedback in real time to ensure accuracy.
- Email intentionally. Assess whether vendors are on a thread who may not need to see what you have to say.
- Likewise, minimize who within an organization is included on communications, including emails and calls. Courts have cited the presence of many different people from within a company as a reason to find against both attorney-client privilege and work product protection.

Authors

This GT Alert was prepared by:

- Jena M. Valdetero | +1 312.456.1025 | Jena.Valdetero@gtlaw.com
- Emily S. Taetzsch | +1 312.236.4328 | Emily.Taetzsch@gtlaw.com