Cybersecurity Law Report cslawreport.com

Jul. 20, 2022

Privilege

# Looking Back on the Breach: Fundamentals of Preserving Privilege of Forensic Analyses in the Wake of a Data Breach

By Alejandro H. Cruz and Elana M. Stern, *Patterson Belknap Webb & Tyler LLP*

The rise of ransomware and other increasingly sophisticated cyberattacks in recent years has made data breaches, large and small, a common and often existential threat to businesses across industries. Such events require both investigative and remedial steps, which include engaging forensic experts and attorneys to prepare for the litigation that has become an inevitable follow-on risk. Questions of privilege and work-product protection routinely arise in post-breach litigation, especially concerning forensic consultants' analyses. Plaintiffs target these materials in discovery because they often provide a roadmap to the attack and include details regarding the victim business's defenses and internal steps taken in response to a breach.

Since privilege and work-product protection issues began to surface in post-breach litigation, courts have grappled with them and reached varying results. Despite the uncertainty and highly fact-dependent analyses that have grown out of the case law, five themes emerge to inform best practices in mitigating the risk of compelled disclosure of work performed in the aftermath of a cyber incident.

See "Steps to Protect Privilege for Data Breach Forensic Reports" (Jan. 27, 2021).

## Attorney-Client Privilege, Work-Product Protection and Third-Party Experts

While cyberattacks are a relatively new context for discovery disputes, attorney-client privilege and work-product protection are not. The attorney-client privilege protects confidential communications between lawyer and client; the purpose of this privilege "is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in

the observance of law and administration of justice."[1] The work-product doctrine protects "tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial."[2]

When responding to a cyberattack suffered by a client, counsel's advice, while legal in nature, is inextricably intertwined with and dependent upon technical know-how beyond the ken of even the most tech-savvy attorney. As one court has observed, "one cannot imagine an attorney providing advice to a company faced with the complex litigation and regulatory issues resulting from a data breach . . . without having a technical expert assist the attorney in investigating the facts."[3]

*United States v. Kovel* is the seminal case addressing the application of privilege when lawyers require assistance from such third-party professionals to best advise a client. There, the court confronted the issue of whether the attorney-client privilege extended to an accountant engaged by the lawyer, holding that communications "while the client is relating a complicated tax story to the lawyer" would come within the privilege because "the presence of the accountant is necessary, or at least highly useful, for the effective consultation between the client and the lawyer which the privilege is designed to permit." Crucial to maintaining privilege over such communications, however, is that they "be made in confidence for the purpose of obtaining legal advice from the lawyer."

See "Attorney-Consultant Privilege? Key Considerations for Invoking the *Kovel* Doctrine (Part One of Two)" (Nov. 16, 2016); Part Two (Nov. 30, 2016).

## Five Lessons for Protecting Post-Breach Forensic Analyses

Certain themes arise with increasing frequency as courts analyze whether a forensic expert's work investigating a data breach may be treated similarly to that of the accountant in *Kovel*. These themes can be instructive to practitioners and clients asking whether such work will be subject to disclosure in post-breach litigation or government investigations.

### 1) Bifurcating the Investigation From Remediation

Any business that falls victim to cyber criminals should first call experienced counsel. One factor courts consistently look at to determine whether legal privileges attach to post-breach forensic reports is the purpose underlying the consultant's work. In general, courts have been more likely to find a forensic expert's report protected where the victim business pursues a bifurcated, or, as some courts refer to it, a "two-track," investigation.[4] This approach effectively divides between post-breach analyses conducted at the direction of counsel in anticipation of litigation, and those prepared for purposes of ending and remediating the intrusion.

The forensic expert retained by counsel will analyze the breach and prepare a report to aid counsel's understanding of the breach's technical aspects and consequences so that counsel may best advise their client in anticipation of post-breach litigation and related issues. At the same time, a separate consultant focused on remediation will address the intrusion and report to the victim re-

garding business-related concerns, such as operational continuity and recovery. Courts have often held that reports created by the experts that counsel retains are protected by the attorney-client privilege and work-product doctrines, and therefore not subject to compelled disclosure in post-breach litigation.

For example, in *In re Target Corp. Customer Data Sec. Breach Litig.*, Target both "conducted its own ordinary-course investigation" and created a second "task force and engaged a separate team . . . to provide counsel with the necessary input." Target claimed that the work of that latter team was both privileged and covered by work-product protection; the court agreed. Similarly, in *Maldondo v. Solara Med. Supplies, LLC*, hackers broke into defendant Solara Medical Supplies' computer system. After discovering the breach, Solara engaged outside counsel, who in turn retained a forensic investigative firm to conduct two separate work streams: one to "provide specialized information to counsel . . . so that attorneys there could give informed legal counsel to Solara," and the second, "walled-off from the first team," was to "prepare a report for the sole purpose of providing the [Federal Trade Commission] with additional information . . . ." (quotations omitted). The court denied plaintiffs' motion to compel production of the materials from the first investigation, finding them "privileged under the work product doctrine or the attorney-client privilege."

Where, as in *In re Experian Data Breach Litigation*, outside counsel, and not the victim business itself, retains a forensic expert to conduct the post-breach investigation and prepare a report, and the "purpose of that report is to help [counsel] provide legal advice to [the victim business] regarding the attack," courts have denied motions to compel production of such reports.[5]

After suffering a data breach, Experian hired a law firm, and the law firm hired third-party forensic consultant Mandiant to investigate the breach and prepare a report. In denying the plaintiffs' motion to compel discovery of Mandiant's report, the court focused on the fact that Mandiant "conducted the investigation and prepared its report for [counsel] in anticipation of litigation, even if that wasn't Mandiant's only purpose."

Similarly, in *Karter v. Epiq Systems, Inc.*, the court held that the forensic consultant's report was protected by the work-product doctrine where counsel hired the consultant firm, "and [] it was not the firm that was primarily involved in trying to get the computers back up and running; but rather, was being retained to give advice in anticipation that there would be data-breach litigation."[6]

For purposes of privilege and work-product protection, counsel's involvement in the investigation must go beyond merely retaining the third-party forensic consultant. In *Guo Wengui v. Clark Hill*, although defendant Clark Hill had hired outside counsel who in turn hired a forensic consultant, the court found that "Clark Hill papered the arrangement using its attorneys" in order to "help shield material from disclosure and [that] is not sufficient in itself to provide work-product protection." (quotations omitted). According to the court, the consultant's work in *Guo* overlapped with remediation; it was "far broader than merely assisting outside counsel in preparation for litigation."

Similarly, in *In re Premera Blue Cross Customer Data Security Breach Litigation*, the court concluded that a "change of supervision [to outside counsel], by itself, is not sufficient to render all of the later

communications and underlying documents privileged or immune from discovery as work product." Relatedly, when the victim business itself – instead of outside counsel – retains a forensic expert to conduct a single post-breach investigation, courts are more likely to conclude that the expert's work was performed for a business purpose – as opposed to in anticipation of litigation or in aid of legal advice – and is therefore discoverable.[7] In short, retaining the expert is not enough: counsel must, in fact, be involved in the investigation to help maintain its distinction from any separate work focused on remediation.

See "*Target* Privilege Decision Delivers Guidance for Post-Data Breach Internal Investigations" (Nov. 11, 2015).

## 2) Timing and Scoping the Expert's Work

In addition to the structure of the consultant's work, the timing of the consultant's engagement and the relevant scope of work matter. For example, in *Premera*, the victim business engaged a cybersecurity consultant prior to relevant breach. There, and in similar cases, courts have held that the expert's work could not have been performed in anticipation of litigation because the event precipitating litigation – the breach – had not occurred at the time of engagement. In such cases, the forensic experts' reports were held to be discoverable.

In *In re Dominion Dental Servs. USA, Inc. Data Breach Litigation*, for example, defendant businesses hired Mandiant "far before the data breach was discovered," and executed a contemporaneous statement of work with Mandiant and outside counsel that "contemplate[d] incident response services, including: computer incident response support, digital forensics support, advanced threat actor support, and advanced threat/incident assistance." (quotations omitted). After a data breach, a new statement of work was executed, but, according to the court, it contained "virtually identical" deliverables.

The court concluded that the Mandiant report at issue was not protected work-product because, among other reasons, Dominion had engaged Mandiant prior to the breach – and therefore before any threatened litigation – and then entered into an "almost identical" statement of work after the breach occurred. Other courts have come to similar conclusions on comparable facts.[8] While these decisions create a standard that is difficult to meet as a practical matter, they put a premium on engaging a separate consultant to conduct an independent post-breach investigation, with an appropriately tailored scope of work, at the direction of counsel.

## 3) Limiting Access to the Report

Who is given access to the expert's report is also important. Where a post-breach report is shared widely within or beyond the victim business, courts are more likely to determine that any privilege applicable to the report has been waived and that it is therefore subject to discovery. In *Guo*, for example, the report at issue "was shared not just with outside and in-house counsel, but also with se-

lect members of [the defendant's] leadership and IT team," as well as with the FBI. The court denied the application of any privilege or work product protection, noting the report's wide dissemination "for a range of non-litigation purposes." Other courts have held similarly where a forensic expert provided a report to the defendant business and there was "no evidence that it was provided first to [outside counsel]."[9] By contrast, where a report is "not widely disseminated,"[10] and its disclosure is "very limited and closely controlled by" outside and in-house counsel,[11] courts have found such reports protected from discovery.

## 4) Creating and Preserving Contemporaneous Records

Courts have considered victim businesses' maintenance of contemporaneous records related to a breach among the bases to deny discovery into the victims' experts' forensic analyses.[12] In *Experian*, the plaintiffs argued that they were entitled to Experian's forensic expert's report under the "substantial hardship exception" to the work product doctrine.[13] Experian, however, had imaged its servers, and its expert relied on those server images. The court reasoned that because the plaintiffs could obtain the server images in discovery, and retain their own expert to analyze them, the plaintiffs were not entitled to a copy of Experian's consultant's report. The *Karter* court similarly concluded that the plaintiff was not entitled to the defendant's expert's report where the underlying "data has been adequately preserved and [] it can be reviewed by Plaintiff's expert."

## 5) The Non-Testifying Expert Rule

Where a forensic expert is hired to conduct a post-breach analysis and that vendor is shown to be a "non-testifying expert" within the meaning of Rule 26(b)(4)(D), Fed. R. Civ. P., the report may not be subject to discovery. The non-testifying expert rule is "distinct from" privilege and work-product doctrines.[14] Rule 26(b)(4)(D) provides, in relevant part, that "[o]rdinarily, a party may not, by interrogatories or deposition, discover facts known or opinions held by an expert who has been retained or specially employed by another party in anticipation of litigation or to prepare for trial and who is not expected to be called as a witness at trial."

An exception exists where the party seeking discovery can show "exceptional circumstances under which it is impracticable for the party to obtain facts or opinions on the same subject by other means."[15] Some "courts have found exceptional circumstances where the object or condition at issue cannot be observed by experts of the party seeking discovery."[16] But where the same information the non-testifying expert relied on – such as the underlying forensic data – is available to an opposing party in discovery, the "exceptional circumstances" carve-out may not be met.[17] This further underscores the importance of counsel engaging forensic experts; counsel should carefully consider the capacity in which such a consultant is retained because additional protections may attach to a non-testifying expert's work.

## The Upshot: Mitigating the Risk That a Post-Breach Forensic Report Will Be Discoverable

There is no one-size-fits-all response to a cyber incident and preserving the protections that may apply to post-breach forensic analyses will likely remain an area of uncertainty. The following practices may help maximize the protection afforded to such work in follow-on litigation:

1. **Cyberattack victims and their counsel should ensure that counsel directly engages any forensic expert to conduct an investigation for purposes of advising the client and defending against resultant litigation and investigations**. Bifurcating the post-breach response will help ensure that non-privileged remediation work is separate from investigative work in anticipation of litigation and in aid of advising the client as to its breach-related legal obligations. Maintaining such separate, parallel tracks will help show division between privileged communications and/or protected work product on the one hand, and work that may be perceived by courts as business-related, and therefore discoverable, on the other.
2. **The forensic expert working on the investigation should be retained by counsel exclusively to investigate the breach, with a written statement of work that reflects the specific scope of the engagement**. In addition to an engagement letter and carefully tailored statement of work, to the extent practicable, a vendor that is already performing ongoing data security or incident response work for the victim business at the time of the breach should not also be tasked with investigating the breach.
3. **A forensic report generated at the direction of counsel should only be shared on a "need-to-know" basis, with a limited group of people**. That group of people may include, for example, outside counsel and the victim business's in-house counsel. Clients should consider additional measures to ensure limited and monitored distribution, including only distributing numbered, hard copies of the report, keeping detailed records of who receives the report and for what reason, and instructing those who receive the report to store it in a secure location and not to make copies or otherwise share it.
4. **Preserve data and information underlying the work and analysis of any retained forensic consultant**. The subsequent availability of these records in litigation may defuse arguments by an opposing party based on a purported substantial need for the resulting forensic reports.
5. **Counsel should consider the potential applicability of the non-testifying expert rule under appropriate circumstances**. The availability of non-testifying expert protections may depend on many of the same considerations discussed above, including segregating post-breach investigative work at the direction of counsel, limiting the scope of a forensic expert's work, and maintaining the data underlying any litigation-focused analysis.

Cyberattacks of any kind take their victims down a path fraught with risk and uncertainty. However, implementing these lessons from nearly a decade of developing law may help businesses and their counsel reduce the risk that broad swaths of post-breach forensic work become subject to disclosure.

*Alejandro H. Cruz is a partner in Patterson Belknap Webb & Tyler LLP's litigation department. His practice is focused on complex commercial litigation and government investigations, cybersecurity and incident response, and defense of professional malpractice actions.*

*Elana M. Stern is an associate in Patterson Belknap Webb & Tyler LLP's litigation department. Her practice focuses on complex commercial matters.*

[1] *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

[2] Fed. R. Evid. 502(g)(2); *Hickman v. Taylor*, 329 U.S. 495, 510-11 (1947).

[3] *Maldondo v. Solara Med. Supplies, LLC*, No. 20-12198-LTS, 2021 WL 8323636, at *4 (D. Mass. June 2, 2021).

[4] *In re Target Corp. Customer Data Sec. Breach Litig.*, MDL No. 14-2522, 2015 WL 6777384, at *2 (D. Minn. Oct. 23, 2015); *Maldondo*, 2021 WL 8323636, at *4-5.

[5] *In re Experian Data Breach Litig.*, No. SACV 15-01592 AG, 2017 WL 4325583, at *2 (C.D. Cal. May 18, 2017); *Maldondo*, 2021 WL 8323636, at *4-5.

[6] Patterson Belknap Webb & Tyler LLP attorneys represented defendant Epiq Systems in this litigation.

[7] *See In re Premera Blue Cross Customer Data Security Breach Litigation*, *296 F. Supp. 3d* 1230, 1245 (*D. Or.* 2017); *Guo*, 338 F.R.D. at 12-14.

[8] *See, e.g.*, *Premera*, 296 F. Supp. 3d at 1245-46; *In re Capital One Consumer Data Sec. Breach Litig.*, No. 19md2915, 2020 WL 2731238, at *4-7 (E.D. Va. May 26, 2020).

[9] *In re Rutter's Data Sec. Breach Litig.*, No. 20-CV-382, 2021 WL 3733137, at *3 (M.D. Pa. July 22, 2021).

[10] Mot. to Compel Hr'g Tr. at 28, *Karter v. Epiq Sys., Inc.*, ECF No. 87.

[11] *Experian*, 2017 WL 4325583, at *3.

[12] Mot. to Compel Hr'g Tr. at 28-29, *Karter v. Epiq Sys., Inc.*, ECF No. 87; *Experian*, 2017 WL 4325583, at *3.

[13] *Experian*, 2017 WL 4325583, at *3; *see* Fed. R. Civ. P. 26(b)(3)(A).

[14] *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 189 (M.D. Tenn. 2014).

[15] Fed. R. Civ. P. 26(b)(4)(D)(ii).

[16] *Genesco*, 302 F.R.D. at 190 (quotations omitted).

[17] *Id.* at 189-90; *cf. Experian*, 2017 WL 4325583, at *2-3.