Professional Perspective

Maintaining Privilege Over Forensic Reports

Matthew D. Krueger, Eileen R. Ridley, Aaron K. Tantleff, and Jennifer L. Urban, Foley & Lardner

Bloomberg Law

Maintaining Privilege Over Forensic Reports

Contributed by Matthew D. Krueger, Eileen R. Ridley, Aaron K. Tantleff, and Jennifer L. Urban, Foley & Lardner

Following a ransomware attack or other cybersecurity incident, the company whose data has been targeted typically hires—either on its own or through outside counsel—a computer forensics examiner to investigate and report on the cause and scope of the incident. In ensuing litigation, companies have successfully shielded these forensic reports from disclosure under the work product doctrine or attorney-client privilege. Several recent court opinions, however, have rejected these claims of privilege.

Moving forward, counsel should understand the rationale underlying these decisions, educate courts about the realities of cybersecurity, and adopt best practices to fortify privilege defenses in future litigation.

Privilege Lost

A recent decision from the U.S. District Court for the Middle District of Pennsylvania underscores the challenges in protecting forensic reports from discovery in litigation following a cyber incident.

The decision, *In re Rutter's Data Security Breach Litigation*, 2021 BL 275161 (July 22, 2021), addressed a forensics report prepared by Kroll Cyber Security, LLC as part of its investigation of a suspected data security incident that hit Rutter's Inc., the convenience store chain. The court rejected Rutter's claims of work product and attorney-client privilege.

Work Product Doctrine

The work product doctrine protects documents prepared by or on behalf of attorneys in anticipation of litigation. The doctrine does not protect reports created for other business purposes—such as preventing future cyber incidents, ensuring business continuity, or offering cybersecurity (as opposed to legal) advice.

In rejecting defendant's assertion of the work product doctrine, the *Rutter's* court focused on three factors: the statement of work (SOW) between Rutter's and Kroll, the deposition testimony of Rutter's representative, and Kroll's delivery of the report directly to Rutter's.

First, the court construed the SOW as indicating that the investigation's purpose was to determine *whether* a breach had occurred, not to prepare for litigation. The court noted that the SOW's description of services section expressly stated: "The overall purpose of this investigation will be to determine whether unauthorized activity within the Rutter's systems environment resulted in the compromise of sensitive data, and to determine the scope of such a compromise if it occurred." The court concluded that such "language demonstrates that Defendant did not have a unilateral belief that litigation would result at the time it requested the Kroll Report."

As for the deposition testimony, Rutter's representative stated that litigation was not contemplated at the time Kroll prepared its forensics report and that Kroll would have prepared the report regardless of the potential for litigation. In fact, the Rutter's representative testified that he was unaware of anyone at Rutter's anticipating litigation when the investigation was requested.

Lastly, the court noted that Kroll's delivery of the forensics report directly to Rutter's, rather than to outside counsel, distinguished this case from others applying the work product doctrine. Sharing the report with non-attorneys gives rise to the presumption that the report's primary purpose was not for assistance in rendering legal advice.

Attorney-Client Privilege

Attorney-client privilege shields communications between client and counsel made in confidence for the purpose of obtaining or providing legal assistance. The privilege also covers communications when a person other than the lawyer is present if that additional person is needed to make the communications possible or to assist the attorney in providing legal services. *Miller v. Haulmark Transp. Sys.*, 104 FRD 442, 445 (E.D. Pa. 1984).

In declining to apply the attorney-client privilege, the *Rutter's* court noted that while the Kroll report did offer solutions for remediating potential vulnerabilities, such advice could not be regarded as legal advice since Kroll personnel were not

professionals in the field of law. The court found that the report was otherwise factual, as Kroll was engaged to monitor and collect data from Rutter's computer equipment, determine the scope and extent of the compromise, and work alongside Rutter's IT personnel to identify and remediate potential vulnerabilities. The court thus concluded: "The record shows that the report and communications were either factual in nature or, where advice and tactics were involved, did not include legal input."

Deciding Factors

Unfortunately for victims of cyber incidents, *Rutter's* narrow view of privilege has prevailed in several other decisions as well. These decisions arguably reflect an unrealistic view of how businesses need to prepare for and respond to cyber incidents. Nevertheless, the opinions address the fundamental question—whether the forensic report facilitated legal advice or a business purpose—by focusing on a variety of factors.

Involvement of Outside Counsel

When the company itself—rather than its outside counsel—retains the computer forensic examiner, the report is less likely to be covered by the work product doctrine. See, e.g., *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1245 (D. Or. 2017). In contrast, work product is more likely to apply when the company hires outside counsel first, documents the anticipation of litigation, and permits outside counsel to hire the forensic examiner, receive the report, and control the report's distribution. See *In re Experian*, 2017 BL 351985 (C.D. Cal. 2017).

Engagement Agreement With Forensic Examiner

Application of the work product doctrine regarding a forensic report may be challenged where the agreement with the forensic examiner fails to demonstrate that the engagement was undertaken primarily because of potential litigation. Some courts have given only minimal weight to headers on the forensic examiner's reports stating they are "privileged," "work-product," "at the request of counsel," or "under the direction of Counsel." *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d at 1245; *In re Dominion Dental Servs. USA, Inc. Data Breach Litig*., 429 F. Supp. 3d 190, 194 (E.D. Va. 2019).

Similarly, some courts have assessed whether the agreement's scope of work mirrors earlier agreements with the forensic examiner conducted for general business purposes. See, e.g., *In re Capital One Consumer Data Sec. Breach Litig.*, 2020 BL 195019 (E.D. Va. May 26, 2020); *In re Dominion*, 429 F. Supp. 3d at 194; *In re Premera*, 296 F. Supp. 3d at 1245.

Prior Relationship With Forensic Examiner

If a company has an outside-managed security service provider and asks it to conduct the forensic examination, a court may be less likely to find that the work product doctrine applies to the post-incident report unless there is a history establishing that the investigation was undertaken in contemplation of litigation. That ongoing business relationship may suggest that the report was prepared for general cybersecurity or business purposes rather than for potential litigation. See, e.g., *In re Capital One*, 2020 BL 195019; *In re Dominion*, 429 F. Supp. 3d at 194; *In re Premera*, 296 F. Supp. 3d at 1245.

However, a previous engagement of the computer forensic examiner should not preclude a claim of work product privilege when outside counsel hires the same examiner post-incident, and the circumstances show that the examiner was asked to conduct an examination for potential litigation. See *In re Experian*, 2017 BL 351985. Indeed, counsel need to educate courts that it is best to engage a forensic examination firm before an incident in accordance with the company's incident response plan, so as to act quickly and responsibly after an incident.

Payment of Forensic Examiner

Several courts have analyzed whether payment for the examiner came from an existing retainer or legal funds. *In re Capital One*, 2020 BL 195019.

One court highlighted that the forensic provider's fees came from the cybersecurity budget, rather than from legal, as indicating that the company did not retain the forensic provider to facilitate legal advice. *Wengui v. Clark Hill*, 2021 BL 9415 (D.D.C. Jan. 12, 2021). However, that factor should not be given much weight. Businesses use a wide variety of accounting and budgetary structures, and charging one division's budget over another does not necessarily reflect whether litigation is anticipated.

Scope of Forensic Report

If the examiner's report only contains information that counsel will need to prepare for litigation or give legal advice, the privilege is more likely to apply.

In *Wengui*, by contrast, the forensic examiner's report included "pages of specific recommendations on how Clark Hill should tighten its cybersecurity." *Wengui v. Clark Hill*, 2021 BL 9415 (D.D.C. Jan. 12, 2021). The court held that the attorney-client privilege did not apply on the grounds that those recommendations reflected advice for future cybersecurity rather than legal advice regarding the prior incident.

Conversely, reviewing and implementing remedial measures may also be construed in the context of preparation for litigation—e.g., minimizing suits, etc. Accordingly, there may be justifiable reasons for including information regarding specific remedial measures. However, when doing so, it is best to state and support the purposes for doing so. Indeed, counsel must help courts understand that remediation is often part-and-parcel of preparing for litigation.

Maintenance of Confidentiality

Excessive disclosures of the underlying report may cut against claims that a forensic report is attorney work product.

In the *Capital One* decision, the court held the forensic report did not qualify as attorney work product in part because the report was shared with Capital One's Board of Directors, approximately fifty Capital One employees, four regulators, and an accounting firm. *In re Capital One*, 2020 BL 195019.

In an even stingier decision, the *Wengui* court refused to protect the forensic report because it was shared "not just with outside and in-house counsel, but also with 'select members of Clark Hill's leadership and IT team.'" *Wengui v. Clark Hill*, 2021 BL 9415 (D.D.C. Jan. 12, 2021).

Conversely, Experian did not waive the protection when outside counsel limited disclosure to in-house counsel, did not provide the full report to Experian's Incident Response Team or remediation personnel, and only provided a redacted form of the report to T-Mobile's counsel under a joint defense agreement. See *In re Experian*, 2017 BL 351985 (C.D. Cal. 2017).

Use of Two-Track Post-Incident Investigation

Some companies have sought to maintain work-product protection by commissioning two separate investigations that result in two distinct forensic reports—one for litigation and the other for business purposes.

For example, in *Target*, the company performed its own independent data breach investigation to learn how the breach happened, how they should remediate the incident, and how they should respond. See *In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 BL 369979 (D. Minn. Oct. 23, 2015). Target produced the resulting report in discovery.

Target's outside counsel conducted a second, separate investigation and retained a computer forensic expert to assist counsel in providing legal advice to Target in connection with the data breach. This second report was successfully withheld from opposing counsel in litigation.

It bears noting that Target's data breach involved Payment Card Industry (PCI) data, which often requires a separate PCI forensic investigation (PFI).

Relying on the *Target* decision, Clark Hill's counsel argued that a similar two-track investigation had been employed in that case, and that plaintiff was not entitled to see the report of the second examiner, who had been hired by outside counsel. The court, however, found little support in the record for Clark Hill's "two-track story." Clark Hill produced no evidence showing that the first examiner had conducted a separate investigation with the purpose of "learn[ing] how the breach happened" or facilitating an "appropriate[]" response. *Wengui v. Clark Hill*, 2021 BL 9415 (D.D.C. Jan. 12, 2021). The *Clark Hill* court's rationale is dubious, however: By its very nature, a proper dual-track investigation will commonly result in some overlap of efforts and findings.

It should be noted that the practice of having parallel reports is not an industry standard nor significant factor in the case law. Two-track investigations most frequently deal with larger breaches, given the costs of the procedure. Indeed, the absence of parallel reports should not be taken as an indication that the sought-after report was not prepared for litigation.

Best Practices to Maintain Privilege

Given the fact-intensive analysis courts employ to assess privilege claims for post-incident forensic reports, companies should consider the following practices to increase the chances of maintaining privilege over post-incident forensic reports.

Establish an Incident Response Team

As part of your incident response plan, determine in advance who your incident response counsel and computer forensic examiner will be, and clear them beforehand with your cyber insurer. Incident response counsel should include attorneys engaged for the purpose of handling litigation, and those attorneys should work with the forensic team.

Use an Independent Forensic Provider

If your company uses an outside-managed security service provider, consider selecting a different computer forensic examiner for incident response purposes. Note that findings from an incumbent provider may be less objective, as the provider is unlikely to consider itself as having contributed to the incident

Also consider excluding forensics and incident response services from the scope of your service provider agreement. Unless expressly excluded, incident response services could be viewed as in the ordinary course of business.

Engage Outside Counsel to Manage Incident Response

When an incident happens, engage outside counsel immediately. Outside counsel should retain your preferred computer forensic examiner and expressly state that the engagement is in anticipation of litigation and to assist in providing legal advice. If outside counsel is engaging a forensic examiner with whom you have an existing relationship, ensure that a new service agreement or statement of work specific to the forensic investigation is used. Ensure that the forensic examiner interfaces with outside counsel rather than directly with your company. Outside counsel should define the scope and purpose of the investigation and be the first to receive the forensic report.

Avoid Using the Same Agreement for Business & Legal Purposes

If you have already engaged a computer forensic examiner in response to an incident, work with your outside counsel to document the work the examiner has done and shared thus far. Outside counsel should then enter into a separate agreement with the examiner with a modified scope following the abovementioned principles.

Consider Paying for Forensics From the Legal Budget

If a forensics examiner is being used to aid in the provision of legal advice, consider paying for such expenses out of the legal budget, rather than IT's or another department's.

Maintain Confidentiality; Limit Distribution

Maintain confidentiality of the forensic report, limiting distribution to those who need to know and only disclosing redacted portions or summaries where possible. With the guidance of outside counsel, limit the distribution and disclosure of attorney-work product only where needed for anticipated litigation or legal advice.

Consider Whether a Written Report Is Necessary

Before a written report is prepared, consider, in consultation with counsel, whether requesting one is appropriate. The agreement with the forensic provider need not include a report as an engagement deliverable. Instead, consider noting that a written or oral report may be prepared and delivered upon the affirmative request of counsel.

Develop a Non-Privileged Report

Almost every incident either requires or would benefit from the sharing of information stemming from the forensic investigation. Various third parties, including board and management members, external auditors, customers, business partners, insurance adjusters, regulatory authorities—and plaintiffs in the event of litigation—are all parties that may seek access to information related to the incident. Accordingly, counsel may be in the best position to create a second, non-privileged report shared with such parties. In contrast, the privileged report may include additional content that would be useful for providing legal advice.

Consider Limiting Forward-Looking Advice

Consider restricting or excluding forward-looking cybersecurity recommendations from the report, as these may not be considered legal advice. Further, consider the impact of including any recommendations that are ultimately not implemented by the company. Note, however, that privilege may still apply if the remediation measures are prescribed to assist outside counsel in preparing for litigation—e.g., by showing mitigation measures.

Always Consider the Possibility of Disclosure

While the forensic report and the attorney-work product prepared in anticipation of litigation is generally drafted with the expectation of remaining protected from disclosure, there is always the possibility of the report's disclosure. Consider the potential for discovery in litigation when drafting the report—whether the final report, interim drafts, and commentary thereon. Be thoughtful in drafting.

Consider a Dual-Track Investigation

Depending on the circumstances, consider creating a dual-track investigation, with one track focusing on operations and the other focusing on legal. This may require retention of two separate forensic providers or two independent teams from the same provider. The operational team may be focused on investigating the source of the security incident and remediating its cause, working with the internal IT team.

In contrast, the legal track, retained by counsel, provides information directly to counsel to aid in providing legal advice to the company. This may help define the separation of privileged and non-privileged information. As noted, however, this is not the industry standard, nor should this be viewed as required to keep the privilege.

Engage Foreign Counsel for Cross-Border Incidents

Each jurisdiction and country have different rules and procedures for protecting attorney-client communications and work-product, in addition to other differences that may impact the legal considerations of a data incident in a given jurisdiction. Thus, local counsel would advise on how best to protect privilege in such jurisdictions.

In sum, this area of law is evolving, and there is no way to guarantee the protection of the forensic report from discovery. However, following the above practices should enhance the chances that work product and attorney-client defenses withstand motions to compel.

With assistance from Paige M. Papandrea, Avi B. Ginsberg, Steven M. Millendorf, and Ruba Assaf (a 2021 Foley & Lardner summer associate).

