3 Ways To Shield Cyber Reports After Clark Hill Breach Ruling

By **Colin Jennings and Ericka Johnson** (January 21, 2021)

Colin Jennings

Ericka Johnson

On Jan. 12, a district judge in the U.S. District Court for the District of Columbia ordered Clark Hill PLC to produce a forensic report prepared by the cybersecurity firm Duff & Phelps, holding that the report was not protected as attorney work product despite having been prepared at the direction of counsel.

Accordingly, Wengui v. Clark Hill appears to be the next case in the continuing saga over how and the extent to which a forensic report can be protected from discovery. A forensic report is normally prepared by a cybersecurity firm, at the direction of outside counsel, following a thorough investigation into the nature and scope of a defendant company's cyberattack.

Although most would instinctively think that such a report is privileged, this decision seems to build on a series of cases holding otherwise. For example, the decision in the U.S. District Court for the Eastern District of Virginia case In re: Capital One Consumer Data Security Breach Litigation last year determined the forensic report was discoverable.

The discoverability of a forensic report is a very significant issue because it will generally detail the critical vulnerabilities in a company's information technology environment that enabled the cyberattack, often identifying areas in which a company's IT defense were not compliant with best practices, regulators and/or industry standards — in other words potential evidence of negligence or recklessness that would not otherwise exist but for the forensic report.

In the present matter, plaintiff Guo Wengui accused his former law firm, which he had hired to prepare his U.S. asylum application, of recklessly allowing his political enemies to steal his confidential information during a 2017 cyberattack. To identify evidence of recklessness, among other things, Wengui moved to compel Clark Hill to produce all reports of its forensic investigation into the cyberattack.

While it is beneficial to counsel to anticipate and defend against potential causes of action, plaintiffs like Wengui will seek to discover forensic reports as evidence to substantiate their claims. Therefore, forensic reports have become hotly contested during breach litigation, leading to evolving best practices to protect a report from becoming discoverable.

In determining whether a forensic report is privileged, courts will look to the totality of circumstances to determine whether a forensic report was truly created in anticipation of litigation. As the next case to weigh in on the best practices to establish privilege over a forensic report, Wengui provides three key takeaways.

1. Consider conducting a two-track investigation.

The Capital One decision last year made it clear that companies should ensure their outside counsel retains a cybersecurity vendor with which it has no preexisting relationship for incident response services, finding that to truly anticipate litigation, the scope of the forensic services must be determined after the cyberattack.

However, it may not be feasible to engage a cybersecurity firm with no preexisting relationships.

Additionally, a company may require the findings of a forensic investigation for business considerations, e.g., determining profit or liability projections, identifying software or hardware upgrades, liaising with the FBI for attribution purposes. Under these circumstances, a company should consider creating a two-track investigation: one privileged investigation in anticipation of litigation and the other nonprivileged investigation for business purposes.

In Wengui, Clark Hill argued that the Duff & Phelps report was only one-half of a two-track investigation, where Clark Hill's existing vendor, eSentire Inc., conducted a separate, nonprivileged investigation for business purposes. Accordingly, Clark Hill argued, it had produced eSentire's nonprivileged work product while appropriately withholding Duff & Phelps' privileged report.

The court appeared persuaded by Clark Hill's argument that it should apply the same ruling as under In re: Target Corp. Customer Data Security Breach Litigation. In that case, Target conducted a two-track investigation, and the court ruled that Target appropriately withheld the forensic report created in anticipation of litigation.

Unfortunately for Clark Hill, the court found that the record did not support the existence of a two-track investigation. The court noted that the closest Clark Hill came was an equivocal statement by its director of information security, that "[b]ecause of eSentire's work, Clark Hill did not need the Duff & Phelps report for business continuity."

Accordingly, Wengui is consistent with Target, finding that a two-track investigation provides strong evidence that a report was created in anticipation of litigation. As a practical matter, a company can leverage its existing third-party IT provider or cybersecurity firm with a preexisting relationship to conduct an investigation for business purposes while retaining a cybersecurity firm, at the direction of outside counsel, to conduct an investigation in anticipation of litigation.

2. Use the report only for litigation purposes, and limit its disclosure to the in-house counsel.

A company should use the forensic report solely for litigation purposes and should limit is distribution to only those who absolutely need it for these purposes. Such individuals may include the in-house counsel and possibly one or two cybersecurity employees who need to understand the full nature and scope of the attack and the vulnerabilities identified to assist counsel in the assessment of potential claims and defenses.

In Capital One, the court emphasized that about 50 employees, four regulators, an accounting firm and a corporate governance general email box received a copy of the forensic report in finding that the report was not protected by the attorney work product doctrine.

However, Wengui is more restrictive than Capital One. In Wengui, the court noted that the report was only shared with select members of Clark Hill's leadership and IT team, as well as with the FBI to assist its investigation of the cyber incident. Notwithstanding the limited distribution, the Wengui court still found that this was evidence that the report was not created in anticipation of litigation, but for business and investigative purposes.

Accordingly, based on Wengui, the safest course of action is to provide the full report only to the in-house counsel. As a practical matter, in-house counsel can share, as necessary, a high-level summary of the report to third parties such as auditors, law enforcement and boards of directors. This will ensure that the report's detailed analysis related to the nature and scope of the attack remain privileged.

3. Do not include recommendations for remediation in a forensic report.

Outside counsel should ensure that a forensic report does not contain recommendations to strengthen a company's IT environment. Generally, materials prepared in the ordinary course of business or pursuant to regulatory requirements are not documents prepared in anticipation of litigation.

In Wengui, the court emphasized that the forensic report provided "pages of specific recommendations on how Clark Hill should tighten its cybersecurity," which was shared with both Clark Hill IT staff and the FBI. The court noted that the report was provided "presumably with an eye towards facilitating both entities' further efforts at investigation and remediation."

The court further distinguished Target from the present matter because "the Target court specifically noted that the relevant investigation and report were not 'focused … on remediation of the breach.'" Accordingly, the court concluded that Clark Hill's true objective was gleaning Duff & Phelps' expertise in cybersecurity and not obtaining legal advice from its lawyers.

Wengui is therefore consistent with Target. As a best practice, companies should ensure that the forensic report does not include recommendations for remediation. As a practical matter, forensic firms often create standalone documents related to short and long terms steps companies must take to contain an incident to mitigate the risk of a reattack.

Colin Jennings is a partner and Ericka Johnson is an associate at Squire Patton Boggs LLP.