Proskauer

Lessons from Wengui v. Clark Hill: Structuring a Two Track Cyber Investigation

Minding Your Business Blog on **February 8, 2021**

As the D.C. District Court in *Wengui v. Clark Hill* recently commented, "[m]alicious cyberattacks have unfortunately become a routine part of our modern digital world. So have the lawsuits that follow them…." The court's decision in that case has added another data point to developing jurisprudence of the cyberattack landscape, specifically concerning the discoverability of post-breach forensics reports.

A former client of the Clark Hill law firm sued the firm for failing to protect his confidential information after a hacker stole the client's data from the firm's systems. The former client moved to compel the firm to produce all reports relating to Clark Hill's investigation into the cyberattack. Clark Hill argued that certain materials were protected from discovery because it had initiated a "two track" investigation into the breach, an approach sometimes used by companies following security incidents. Clark Hill claimed that one track was a non-privileged investigation into the breach and the other track was an investigation for legal purposes, and that materials prepared on the legal track were protected from discovery. The court disagreed, noting that Clark Hill failed to show that it had actually conducted a two track investigation. The court also found that the circumstances of the case showed Clark Hill had blurred the non-privileged business track and the legal track in ways meaningful to its privilege determination.

Typically, a two track method can be very useful in cyber investigations that carry a high legal risk because, if structured and executed properly, materials prepared on the legal track have a greater chance of being protected from discovery while documents prepared on the business track can be used for a wide range of purposes. Clark Hill, however, failed to provide evidence that it conducted a two track investigation. Even though Clark Hill set up two tracks, one using its ordinary-course-of-business cybersecurity vendor for business purposes, and the other using a different cybersecurity vendor retained by outside counsel for legal purposes, the court concluded that "Clark Hill turned to [the vendor retained by counsel] *instead of*, rather than *separate from* or *in addition to*, [its ordinary business vendor], to do the necessary investigative work."

Specifically, the court noted that Clark Hill did not provide testimony confirming that its ordinary-course-of-business vendor conducted a separate investigation, much less did Clark Hill provide any evidence that its ordinary business vendor produced any of its own findings. Instead, the court suggested that the two tracks were blurred and pointed to the fact that the report created on the legal track was the only comprehensive report produced, that it included subject matter related to business continuity, such as remediation actions, and that it was distributed to outside and inside counsel, select members of Clark Hill's leadership and IT team, and the FBI for a variety of legal and non-legal purposes.

In short, the decision in *Wengui v. Clark Hill* repeats a theme that other courts that have stressed in the cyberattack context, which is that creating a "papered arrangement using its attorneys" to claim privileges and/or protections over post-breach forensics reports is not enough. To benefit from the two track method, the party claiming the privileges or protections needs to produce enough evidence to show that it actually conducted a two track investigation. The following elements may help counsel a structure their investigation to meet their evidentiary burden:

- Have different people do different things. While the court in *Wengui v. Clark Hill* did not suggest that there needs to be complete separation between the business and legal tracks, there should be enough evidence to show that two investigations were conducted each with a different goal in mind. This can include, for example different teams and minimal overlap of team members.
- Prepare two reports—a factual, business purpose report and a legal purpose report. Again, while both reports may inevitably have content in common, such as

background information about the cyberattack, the reports should each have a different focus. For example, the legal track report can be focused on legal issues such as liability and culpability, rather on remediation actions.

- Manage the distribution of each report. How a report is used and distributed may suggest to a court that it is prepared for a business purpose instead of a legal purpose. A safer course may therefore be to not only create two separate reports, but to strictly limit disclosure of the legal purpose report and limit its use to legal purposes only.

As illustrated by the court's decision, a threshold issue continues to be that "papered arrangements using attorneys," without more is insufficient to protect post-breach forensics reports from discovery in litigation. The more evidence distinguishing the legal track from the business track, the more likely a court will conclude that a two track investigation was conducted and legal track materials to be protected. Companies should therefore continue following the evolving case law and take steps to understand the evidentiary thresholds underlying privilege determinations, so that they can structure investigations that meet their business and legal needs while avoiding costly discovery disputes.

View Original