LAW360®

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Clark Hill Must Produce Cyberattack Report In Malpractice Suit

By **Craig Clough**

Law360 (January 12, 2021, 11:18 PM EST) -- A D.C. federal court granted a Chinese dissident's bid Monday to compel Clark Hill PLC, which used to represent him, to produce a report it commissioned on a cyberattack at the center of the dissident's $50 million malpractice suit, ruling the report is neither protected work product nor attorney-client privileged.

U.S. District Judge James E. Boasberg pointed to various evidence that the report from financial consulting firm Duff & Phelps was used and disseminated by Clark Hill for purposes beyond preparing for litigation or for privileged legal advice, including that it was shared with the FBI and its own IT department.

Using the report for non-litigation purposes "reinforces the notion that it cannot be fairly described as prepared in anticipation of litigation," the judge said in finding it is not a protected work product.

In finding the report is not attorney-client privileged, the judge said he concluded that Clark Hill's "true objective was gleaning Duff & Phelps's expertise in cybersecurity" and not in obtaining legal advice.

Businessman Guo Wengui has accused the firm and its immigration attorney Thomas Ragland, whom he had hired to prepare his U.S. asylum application, of recklessly allowing his political enemies to steal his confidential information.

In the lawsuit, removed from D.C. Superior Court to federal court last fall, Guo said his asylum application was necessitated by a politically motivated persecution by the government of his native China.

Despite Guo's warning to Clark Hill that his foes might try to infiltrate firm computers — and its assurances that precautions were in place — "hostile" actors sponsored by the Chinese government did break in and steal his data in 2017, the suit alleged. That information, which included his entire asylum application, his and his wife's passport numbers and other sensitive information, was then posted online.

The $50 million malpractice suit alleged that the firm's "porous" security measures carelessly allowed the attackers in. Guo also accused the firm of compounding its ethical and legal lapses by abruptly dropping him days after the September 2017 breach by blaming "ethical complications" arising from the possibility that Ragland could be called as a witness in the asylum case.

Guo alleged in his Oct. 21 **motion to compel discovery** that Clark Hill had refused to answer questions about its security systems or the scope of the cyberattack — or even to identify the consultants it hired following the breach.

Clark Hill **argued in a reply brief** in November that Guo's motion was "built on a fallacy," and that the materials he asked for — regarding the firm's cybersecurity policies and practices prior to the data breach, its storage and transmission of his confidential information and its discovery of the attack — have already been provided to him.

Clark Hill said it had conducted two investigations following the cyberattack. In the immediate aftermath, the firm worked with its cybersecurity vendor eSentire Inc. to probe and remediate the attack "as a matter of business continuity," according to the brief. Documents concerning this work have been produced, the firm said.

In the other probe, Clark Hill said it hired Musick Peeler & Garrett LLP to prepare for litigation stemming from the attack, and Duff & Phelps, which later created a report for counsel to provide legal advice. However, materials concerning the work Duff & Phelps performed are privileged information protected by attorney work-product protection doctrine, the brief emphasized.

But Judge Boasberg disagreed with Clark Hill and ordered it to produce the Duff & Phelps report. A second argument by Clark Hill that the report is privileged because it could identify information about its other clients was also rejected, with the judge saying the issue could be resolved through proper redactions.

The judge said the factual record demonstrates the "true objective" of the report was not obtaining legal advice, and that "[a]t a minimum, defendant has not demonstrated that the opposite is true."

"Duff & Phelps undertook a full investigation — the only one apparently commissioned by Clark Hill — with the goal of determining how the attack happened and what information was exfiltrated," he judge added. "The report provides not only a summary of the firm's findings, but also pages of specific recommendations on how Clark Hill should tighten its cybersecurity. And it was shared with both Clark Hill IT staff and the FBI, presumably with an eye toward facilitating both entities' further efforts at investigation and remediation."

Counsel for the parties did not immediately respond to requests for comment.

Guo is represented by Ari S. Casper and Ralph S. Tyler of the Casper Firm LLC.

Clark Hill is represented by John R. Storino, Kali N. Bracey and Leigh J. Jahnig of Jenner & Block LLP.

The case is Guo Wengui v. Clark Hill PLC et al., case number 1:19-cv-03195, in the U.S. District Court for the District of Columbia.

--Additional reporting by Khorri Atkinson. Editing by Bruce Goldman.
