Lowenstein Sandler

The Tech Group
White Collar Criminal Defense

January 21, 2021

Recent Decision Highlights Considerations for Asserting Privilege in the Wake of a Cyberattack

By Kathleen A. McGee and Rebecca J. Ryan

"Malicious cyberattacks have unfortunately become a routine part of our modern digital world." *Wengui v. Clark Hill, PLC*, Civil Action No. 19-3195, slip op. at 1 (D.D.C. Jan 12. 2021). When a data breach occurs, in-house counsel must respond quickly to identify the source of the breach, remediate any damage, and make any required notifications to consumers, customers, and regulators. In the midst of the immediate crisis response, however, in-house counsel and their advisors must also be forward-thinking about the frequently inevitable data security lawsuits and regulator-initiated investigations that follow, including whether documents generated in the wake of the data breach will be discoverable or shielded by the attorney-client or work-product privileges. Typically, third-party vendors (e.g., forensic experts, public relations firms) are engaged through outside counsel to protect these documents from disclosure. A recent decision out of the U.S. District Court for the District of Columbia suggests that plaintiffs and courts are taking a more exacting look at such assertions of privilege.

In *Wengui*, the plaintiff sued his former law firm, which had been the subject of a cyberattack, alleging deficiencies in the measures taken by the firm to safeguard data. *Id*. at 1. In discovery, plaintiff sought all reports of the law firm's investigation into the cyberattack.[1] *Id*. at 1. Among other things, the law firm objected to the production of a report and related documents generated by an outside security consulting firm, hired by outside counsel, as covered by the attorney-client and work-product privileges. *Id*. at 2. The court overruled both objections and granted plaintiff's motion to compel.

First, the court held that the work-product privilege did not apply because the law firm did not meet its burden that the report was prepared or obtained *because of* the prospect of litigation. *Id*. at 4. Put differently, the law firm did not show that the report would *not* have been created in the ordinary course of business, irrespective of litigation. *Id*. at 4-5. The court noted that for many institutions–particularly those that handle sensitive information–determining how a cyberattack occurred is a "necessary business function." *Id*. at 4-5. Indeed, in this case, the record reflected that the report was used by the law firm for a range of non-litigation purposes. *Id*. at 8. Under these circumstances, the court found that "papering" the arrangement using its outside counsel, an approach that "appears to [have been] designed to help shield material from disclosure," was "not sufficient in itself to provide work-product protection." *Id*. at 9 (alteration in original) (citations omitted).

Second, the court found that the documents were not protected attorney-client communications. *Id*. at 12. Extending this protection to reports of third parties is to be applied "narrowly" to situations where a third party, such as an accountant, acts as a translator to assist an attorney in providing legal advice. *Id*. at 10. Here, the court found that the law firm's objective in engaging the third-party vendor was to benefit from its expertise in cybersecurity and not to obtain legal counsel. *Id*. at 11.

[1] The law firm also objected to plaintiff's request that it provide information related to other clients who may or may not have been affected by the at-issue hack. *Id*. at 2. The court found that plaintiff's request for information on the effect of the cyberattack on other firm clients was permissible, as the scope of the attack was relevant to the sufficiency and reasonableness of defendant's cybersecurity at the time of the attack. *Id*. at 12–14.

The *Wengui* decision builds upon growing case law in this area, including a 2017 decision out of the U.S. District Court for the District of Oregon. I*n re Premera Blue Cross Customer Data Sec. Breach Litig*., 296 F. Supp. 3d 1230 (D. Or. 2017). In Premera, the district court also found that documents created by third parties hired by counsel following a data breach were not automatically covered by the attorney-client or work-product privileges. *Id*. 1242-1244. Again, the focus of the court was whether (i) the primary purpose of such materials (such as draft press releases from a public relations firm) was to perform a business function and not to communicate with counsel or obtain legal advice, and/or (ii) the material would have been prepared in the normal course of business and not solely due to a pending suit. *Id*.

Understanding the legal framework under which privilege determinations will ultimately be made can not only guide counsel and their advisors to make informed decisions about how best to structure relationships to protect these privileges but also may help avoid costly discovery disputes. Establishing a risk management protocol that considers privilege will help ensure that an organization's crisis response contains measures and controls for gathering critical information in the most efficient, most secure method possible.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

REBECCA J. RYAN
Associate
T: 973.422.6470
rryan@lowenstein.com