Lessons from Cyber Intrusions: Separation is Key to Ensure Work Product Doctrine Protection

By Leo K. Barnes Jr.

The Covid-related increase in the number of employees working remotely has created an unexpected consequence: heightened risk of cyber intrusions as employees are logging on through their home networks or with personal devices that might not be as secure as office environments. Because it takes the unprotected business 6 months or more to realize that it has been violated, many of the intrusions which have already occurred have yet to surface, likely leading to a spate of ancillary litigation during 2021.

When a lawsuit related to such an intrusion inevitably occurs, counsel's first call will likely be to a cyber-security company that can provide potential expert witness services on the "5Ws" (who, what, where, when and why) concerning the intrusion. Often times, the violated company may not have cyber security services in place prior to the intrusion and the retention of the expert will originate with counsel. But what occurs when a cyber security vendor is already in place, and was providing services, prior to counsel's retention? How does counsel coordinate with an existing vendor to provide expert analysis—which is cloaked by privilege—such that the corresponding reports are shielded from disclosure?

Leo K. Barnes Jr.

Qualifying for the benefits of the Work Product Doctrine is essential to ensure that documents and communications between client and counsel remain shielded from disclosure during discovery. However, New York courts generally disfavor assertions of evidentiary privileges because they shield evidence from the truth-seeking process; as such, these privileges are confined to the narrowest possible limits. Thus, proper formalities must be implemented to avoid the waiver of the protections afforded by the Work Product Doctrine.

The *Capital One* Litigation

In a recent decision from the United States District Court, Eastern District of Virginia, *In re Capital One Consumer Data Security Breach Litigation*, 2020 WL 2731238, the

(Continued on page 27)

Commercial Litigation (continued from page 12)

court stressed the necessity of adhering to these formalities to afford a party the benefit of the Work Product Doctrine. Beginning in 2015, Capital One entered into a Master Services Agreement with FireEye Inc. d/b/a Mandiant ("Mandiant") to provide cybersecurity services to Capital One. Thereafter, Capital One would enter into periodic "Statements of Work" providing for incident response services in the event such services were needed. On Jan. 7, 2019, the relevant Statement of Work was entered into for incident response services in the following areas: computer security incident response support; digital forensics, log, and malware analysis support; and incident remediation assistance. Mandiant would provide a detailed final report covering the engagement activities, results and recommendations for remediation in a written detailed technical document. Significantly, the retainer for such agreement was designated as a "Business Critical" expense, not a "Legal" expense.

Two months later, during March 2019, a data breach occurred when an unauthorized individual gained access to personal information relating to Capital One's customers. In response, Capital One retained counsel to provide legal advice related to the data breach and both Capital One and counsel entered into a Letter Agreement with Mandiant to provide services and advice concerning "computer security incident response; digital forensics; log and malware analysis; and incident remediation." The payment terms were identical to those contained in the Jan. 7, 2019 Statement of Work and the parties agreed in the Letter Agreement to abide by the same terms as the 2015 Master Services Agreement and the aforementioned Statement of Work; however, Mandiant would now work at the direction Debevoise.

Capital One, on July 29, 2019, issued a public statement regarding the data breach and thereafter a litany of lawsuits was filed against Capital One regarding same. Mandiant performed the services outlined in the Letter Agreement, prepared a report detailing the circumstances surrounding the breach and issued its report on Sept. 4, 2019. Payment was made to Mandiant out of the retainer provided to them under the January 2019 Statement of Work and after that was exhausted, they were paid directly by Capital One through the budget for the Cyber organization. In December 2019, these expenses were re-designated as legal expenses. The Mandiant Report was initially sent to counsel, which then provided the report to Capital One's Legal Department, Board of Directors, as well as approximately 50 Capital One Employees, four regulators and the accounting firm, Ernst & Young.

Analysis

The Capital One adversaries filed a motion to compel production of the Mandiant Report. Based on these facts the court found that the Mandiant Report was not protected from disclosure by application of the Work Product Doctrine. The court began its discussion noting that it was "well-established that courts generally disfavor assertions of evidentiary privileges because they shield evidence from the truth-seeking process; as such, they are to be narrowly and strictly construed so that they are confined to the narrowest possible limits consistent with the logic of its principle" and turned to Federal Rule of Evidence 502 which defines the work-product protection as "the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial." The court also noted that the protections are not warranted by the fact that there is litigation but the material must be prepared "because of" litigation.

The court determined that the Work Product Doctrine did not apply here because the Mandiant Report was: (1) substantially similar to the report/services commissioned *prior to the prospect of litigation*; (2) paid for as a "business-critical" expense and not a "legal" expense; (3) widely distributed throughout Capital One for non-legal purposes; (4) used for financial/regulatory reporting purposes, as opposed to distinctly legal purposes; and (5) created in substantially the same form even without the prospect of litigation.

Lessons learned

The foregoing decision provides a roadmap for savvy counsel to guide the retention of an expert while simultaneously preserving applicable privileges from disclosure, including:

- implementing a Kovel retainer agreement;
- keeping legal expenses and business expenses separate;
- assuming a vendor is already in place at the time that the intrusion occurs, consider the retention of an alternative vendor to serve as a potential expert as opposed to utilizing the same vendor for both roles; and
- distributing potential work-product materials only to those on a "need to know" basis incident to the pending litigation.

For many businesses, it is not a matter of if, but when, a cyber intrusion will occur. Counsel for a cyber-violated business will need to serve as the point person directing the global response so to ensure not only that business-related functions are secure, but that important legal protections are not undermined as a result of the same.

Note: Leo Barnes, a member of Barnes & Barnes, P.C., practices commercial litigation and can be reached at LKB@BarnesPC.com.