CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

EPIC
Insurance Brokers & Consultants

CLIENT ADVISORY

ARE FORENSIC REPORTS PRIVILEGED?

CAPITAL ONE DECISIONS – POST-BREACH FORENSIC REPORT NOT PRIVILEGED

In an order rendered on May 26, 2020[1], a Federal Court in Virginia found that a post-breach forensic report prepared by third-party vendor, Mandiant, under the direction of Capital One's outside counsel was NOT protected from discovery under the attorney work-product doctrine. On June 25, 2020[2], the United States District Court for the Eastern District of Virginia, affirmed the May 26th Order. These decisions serve as an important reminder that attorney client privilege is not a given simply because outside counsel is involved. The privilege is fragile and, it is important to remember, the party asserting the privilege bears the burden of proving its applicability. Organizations should carefully consider and prepare for, in advance of a breach event, how they will engage, pay and direct all third-party vendors involved in the response. A review of the Capital One decisions can help organizations with this planning and preparation. Understanding exactly what happened in these decisions is the key to knowing what proactive steps companies can take to help protect forensic reports from disclosure in the event of post-breach litigation.

TIMELINE AND BACKGROUND

In 2015, Capital One entered into a Master Service Agreement (MSA) with cybersecurity consultant Mandiant to perform various cybersecurity consulting services, including incident response services. The MSA was supplemented by periodic "Statements of Work" (SOW) for specific services.

In January 2019, Capital One entered into a new SOW with Mandiant, allowing for 285 hours of service; again, specifically including incident response services. Significantly, the retainer associated with this SOW was designated, by Capital One, as a "business critical" expense.

In March 2019, Capital One experienced a major breach which compromised the data of over 100 million people in the U.S. and 6 million in Canada. Capital One promptly hired a law firm to provide legal advice and assistance in response to the incident.

On July 29, 2019, Capital One announced that on July 19th they discovered the unauthorized access that occurred in March 2019. Between the date of discovery and the public announcement, Capital One and its outside counsel entered into a Letter Agreement that was, in essence, an extension of the January 2019 SOW. The Letter Agreement provided that Mandiant would continue performing services under the terms of the SOW and would provide incident response, forensic and breach remediation services under the direction of Capital One's outside counsel. And, that the deliverables (i.e. the Report) would be provided to the law firm rather than Capital One directly.

In early September 2019, Mandiant issued a written report to Capital One's counsel. Subsequently, the report was widely distributed to 50 other Capital One employees, four regulatory bodies, and an outside accounting firm. It is unclear whether the report was distributed for regular business purposes or for the purpose of the investigation.

Additional Resources:

[1] https://frostbrowntodd.com/app/uploads/2020/06/In-re-Capital-One-Customer-Data-Sec.-Breach-Litig.-E.D.-Va.-May-26-2020.pdf [2] https://www.johnreedstark.com/wp-content/uploads/sites/180/2020/06/CapitalOneOrder2.pdf

PARTNER INSIGHTS

EPIC's Executive Risk and Cyber Team reached out to Karen Painter Randall, Chair of Cybersecurity and Data Privacy at Connell Foley to discuss this decision and its implications. Karen has an extensive background counseling lawyers and law firms, health care entities, financial institutions, and retail clients by providing proactive plans to address the myriad cyber risks they each face.

EPIC: Thank you for taking the time to provide insights into this case. In your professional opinion, what will be some effects of this ruling?

KAREN: Retaining these qualified security vendors is essential because being prepared ensures that the incident will be detected and responded to quickly and efficiently. A quick response allows for preservation of evidence, containment, eradication, and timely notification if necessary. Additionally, it also mitigates loss for both the organization and, ultimately, the consumer.

EPIC: What precautions could organizations take to plan ahead and ensure a forensic investigation is protected by the attorney-client and work product privilege?

KAREN: In responding to a breach, retain outside incident response counsel first to lead the investigation. Counsel should identify, vet and retain the forensic firm. All Statements of Work should define the scope of services to be supplied in anticipation of litigation and that the cost for forensic services are designated as a legal expense. Furthermore, all invoices should be labeled appropriately and submitted through counsel for privilege protection.

EPIC: Any tips on vetting the forensic firm and how to avoid losing the protections of privilege for breach reports?

KAREN: Incident response counsel should make sure that there is no pre-existing relationship with the forensic firm before retaining to assist with the response effort. All agreements must clearly define the scope of forensic services and relationship with counsel. If after consultation with the breach coach, the client makes an informed decision to use the vendor with a pre-existing relationship, a new and separate agreement should be drafted clearly defining the scope of incident response work in anticipation of litigation, relationship with counsel and costs as legal.

EPIC: One of the issues mentioned in the Capital One case is the amount of parties to which it was distributed. How could that risk be mitigated?

KAREN: In the event a privileged report is prepared, limit its distribution to a small internal group on a need to know basis and include confidentiality instructions for maintaining the privilege. Identify those persons who will have access to the report to reflect its limited circulation. Finally, if privileged information is shared with regulators, consider requesting a Non-Disclosure Agreement and Non-Waiver Agreement.

KEY TAKEAWAYS

- **Burden of Proof:** The Capital One decisions discussed above are important reminders about which party bears the burden of proof when it comes to the attorney client privilege as well as what is necessary to satisfy the burden, specifically in the context of post-breach forensic reports. The party asserting the attorney client privilege bears the burden of demonstrating its applicability. If your organization wants to protect a post-breach forensic report, you must be fully prepared to prove the protection is warranted and plan accordingly.

- **Pre-existing/Long-term Relationship:** This was a pivotal fact in the Capital One case. Capital One and Mandiant had a long-standing contractual relationship – one that pre-dated the March 2019 breach event. The Court determined that the services provided by Mandiant before March 2019 breach and those provided in response to the breach were substantially the "same" type of services. Accordingly, the question became, did Mandiant prepare the report as they normally would, independent of a breach? Or did they prepare the report in anticipation of litigation?

- **Legal Expense vs. Business Expense:** Capital One had a retainer agreement with Mandiant. The retainer, at the time it was paid, was designated by Capital One as a "critical business" expense. Capital One attempted to "reclassify" the expense in December 2019 from a "business expense" to a "legal expense". However, the Court was not persuaded by the attempted reclassification. The designation as a "business" expense, at the time it was paid, supported the position that the report was NOT prepared in anticipation of, or in connection with, the litigation.

- **Wide Distribution:** The wide distribution of the report – to over 50 Capital One employees as well as regulators and their outside accountants – suggested the report was prepared for "business" purposes rather than solely in connection with the litigation.