Lessons Learned for Maintaining Attorney-Client Privileged Data Breach Investigation (and other Consultant) Reports

Alysa Z. Hutnik

June 11, 2020

Following a data breach, companies generally launch an investigation to determine the source and scope of the breach. These efforts are often led by in-house privacy, compliance, and/or litigation counsel with an eye firmly planted on the legal claims that might be asserted, or need to be defended, as a result of that breach. Often key to any data breach investigation is an incident response consultant that helps determine the scope and analyzes the causes of a potential breach. Many companies expect that any reports by, or communications with, the consultant would be protected by the attorney-client privilege and/or work product doctrine, which would shield relevant materials from production during any governmental investigations or third-party litigation that arise from the event. Recently, however, a federal court compelled production of just such a breach report and related documents, calling into question the scope of that protection for data breaches and possibly other corporate investigations.

This post discusses the background and rationale that led to the Court's finding and offers our advice concerning steps that should be taken to maximize the potential scope of protection for consultant reports in data breach investigations and other corporate investigations.

Relevant Background

In March 2019, Capital One experienced a data breach where an unauthorized person gained access to consumers' personal information. Several putative consumer class actions were filed and the cases were consolidated in a multi-district litigation currently pending in the Eastern District of Virginia, captioned *In re Capital One Consumer Data Breach Litigation,* Case No. 1:19-md-2915.

Capital One began its data breach preparedness well before the events at issue in the litigation. In November 2015, Capital One retained FireEye, Inc. d/b/a Mandiant ("Madiant") to provide incident response support. A statement of work outlined the tasks to be performed in the event of a breach and Mandiant was paid a retainer.

On July 19, 2019, Capital One confirmed that a breach had occurred and on July 20 it retained outside counsel. Outside counsel then formally retained Mandiant by executing a new letter agreement to provide the same services outlined in the 2015 agreement. After the initial Mandiant retainer was exhausted, its fees were paid first by the company's cyber team, and then transferred to the legal team budget. All of Mandiant's post-breach reports and data were provided via outside

counsel.

In litigation, Capital One withheld Mandiant's report and other relevant documents associated with its investigation on the basis of attorney-client privilege and the work product doctrine.

Business Not Legal Report

On May 26, 2020, the Court granted Plaintiffs' motion to compel and ordered Capital One to produce the Mandiant report and associated data, documents, and communications. The Court found that Capital One had failed to meet its burden of showing the materials were covered by a relevant privilege.

The Court focused on certain facts that framed the relationship as being of a business, rather than legal, nature. In particular, the Court highlighted the following:

- **Business-Designated Fees:** The fees associated with Mandiant's retention were allocated as "Business Critical" and not a "Legal" expense.
- **Business-Characterized Work:** The work performed by Mandiant was consistent with its 2015 retention and was not altered or otherwise directed by outside counsel in the new letter agreement.
- **Business-Managed Relationship:** The Mandiant relationship was managed by Capital One's manager of its cyber security center and not an attorney.
- **Optics Not Persuasive:** During the pendency of the litigation, the expenses were re-designated to the legal budget and control over Mandiant was transferred to outside counsel. However, the Court found that those procedural adjustments did not alter the engagement or scope of work to be performed.
- **Business Use:** The report was used by Capital One for various business purposes that were wholly unrelated to the litigation or the Legal function.
- **Broadly Circulated:** The report was widely circulated beyond outside counsel and those involved with legal or litigation matters for the company, including to Capital One's Board of Directors, at least fifty-one Capital One employees, four regulators (FDIC, Federal Reserve Board, CFPB, and Office of the Comptroller of the Currency), Ernst & Young accountants. Even for its internal distribution (to the legal department and otherwise), Capital One failed to demonstrate that circulation was limited to the narrow scope of individuals necessary to provide legal advice or for purposes of litigation.

Based on the totality of the circumstances, the Court concluded that Mandiant's analysis and report would have been completed, in substantially similar form, regardless of whether there was the prospect of potential litigation.

Implications and Lessons

The potential implications of the Court's decision extend beyond data security to cover other areas where companies rely on experts to analyze issues that could result in third-party litigation. These may include human resources investigations, accounting audits, and product liability/recall decisions. If the investigations, analysis, and advice generated by consultants are not shielded by privilege, it could have a chilling effect on some companies' own diligence efforts, but also makes compliance efforts harder. The *Capital One* decision does not abolish any rights or protections; rather, it shines a

light on the risks of not fully and properly delineating the scope of a company's outside consultants' retention and work.

As a threshold question, companies should consider whether it is necessary to have a consultant prepare a written report at all. If it is, companies' counsel should make a clear record that the report is being requested for the purpose of anticipated litigation or to provide legal advice. In seeking to maximize the protection afforded consultant reports under the attorney-client and work product privileges, including when preparing their data breach investigation or incident response strategy, companies should keep certain key points in mind:

- **Clearly Defined Legal Scope of Work:** Where a consultant has already been engaged and works with the company, the retainer signed at the direction of counsel must clearly define the terms and scope of work as distinct from the previous business relationship.
- **Paid by Legal:** If a consultant is being retained to provide support for legal advice or concerning potential legal claims, that work should be managed and paid for by legal personnel.
- **Narrow Internal Distribution:** Distribution of investigation reports should be limited to those individuals necessary to complete the legal analysis and litigation work.
- **No External Non-Legal Distribution:** Investigation reports should not be distributed to third parties.
- **Track Distribution:** Distribution of investigation reports should be tracked so that limited distribution can be demonstrated.
- **Segregate Legal from Operational Work:** Where business and legal issues or analysis are part of the same investigation, steps should be taken to segregate the legal- and litigation-related work product from business or operational reports and work.

While no protocol is guaranteed to satisfy every court, and each factual situation is unique, these guideposts improve the odds of meeting the burden required to withhold production of a consultant's report.

Should you have any questions concerning these issues or would like advice concerning how to approach the interplay of consultants and privilege, please feel free to contact us.