Cybersecurity Law Report
An Acuris company

cslawreport.com

June 10, 2020

PRIVILEGE

After Capital One Ruling, How Will Companies Protect Forensic Reports?

By Matt Fleischer-Black, *Cybersecurity Law Report*

The federal court in Virginia overseeing the multi-district litigation (MDL) against Capital One Financial Corp. has ordered the company to release the attorney-supervised forensic report that a cybersecurity firm made following the company's massive 2019 data breach. The company had claimed that work-product protection shielded the post-breach report because its outside lawyers from Debevoise & Plimpton had initiated, directed and received the analysis as part of that firm's own investigation about the breach.

Capital One argued that "the Mandiant Report is core opinion work product prepared to help counsel develop its legal theories about the Cyber Incident and strategy for defending litigation" and "should be protected as inviolate."

In its May 26, 2020 order, The U.S. Court for the Eastern District of Virginia concluded instead that Capital One had failed to distinguish Mandiant's post-breach forensic report from what the cybersecurity consultancy would have delivered without litigation looming. The Court ordered the bank to turn over the report to plaintiffs within 11 days.

The ruling is a warning that businesses cannot count on a series of earlier rulings that shielded forensic reports as privileged, Mark Melodia, a Holland & Knight partner, told the Cybersecurity Law Report. "Most of the time in breach litigation, [the protection of forensic reports has] not been a big subject of debate," he said, adding, "Maybe we've gotten a little complacent assuming and thinking that protection will be there."

See "Increased Post-Breach Discovery Turns Spotlight on Privilege" (Mar. 20, 2019).

Debevoise's Steps to Establish Privilege

Capital One hired Debevoise on July 20, 2019, immediately after discovering that cyber attackers had exposed the sensitive data of over 100 million individuals. Debevoise directly retained cybersecurity consultant Mandiant to help the law firm prepare for a tide of litigation. A few days later, the Virginia-based bank announced the data heist, and consumers filed a wave of lawsuits, since consolidated into an MDL.

Debevoise took several steps to cover Mandiant's investigation under its own protected work product. Debevoise's engagement letter specified that it would direct and receive Mandiant's work to render legal advice for litigation. Capital One paid for

the work from its legal budget (after a delay). The bank partitioned off the Mandiant team from its own cyber team's investigation into the breach, Capital One said. The bank has not claimed privilege over that second set of investigative materials, court documents show.

Once Mandiant delivered its report, Debevoise restricted its distribution to Capital One's legal team, which later shared the report with relatively few non-lawyers at the company. In sum, "all of the circumstances surrounding the creation of the Mandiant report support the conclusion that the Mandiant Report is protected work product," the company argued.

See "Capital One Breach Demonstrates Risk of Overlooking Vulnerabilities When Sending Data to the Cloud" (Aug. 14, 2019).

The Court's Rejection of Work-Product Immunity

Not Enough Evidence It Was Molded by Litigation

The privilege standard will protect work product like the cybersecurity firm's breach report, the order noted, only when the document distinctively reflects preparation for litigation. Capital One had a burden to distinguish the forensic analysis's content from what would appear in a report issued for a pure operational purpose, if a lawsuit was not an issue.

Looking for factors to make that distinction, the Court instead saw a paper trail showing similarity. Capital One first hired Mandiant in 2015, paying the cybersecurity company an annual retainer for 285 hours of work after an incident, which it labeled a "business-critical" expense, not a "legal" one. Capital One's "regular business" agreement, entered into before the incident, and a Debevoise-drafted "litigation" contract executed after the breach looked functionally the same, the Court said. It concluded that the bank had "effectively transferred" its Mandiant agreement to outside counsel.

The Court saw two other indicators of a superficial handover of a business function. The bank initially paid Mandiant's post-breach fees with its existing retainer, only later adjusting its budget attribution to legal. Capital One also supplied the Mandiant forensic report to the bank's outside auditor and four different regulators, which the Court regarded as business purposes.

See "Preserving Privilege in Audits and Internal Investigations" (Jun. 3, 2020).

Describing Mandiant's Technical Work Colorlessly

Debevoise's descriptions did not persuade the Court that Mandiant's breach analysis touched sufficiently on legal elements, impressions, or other traditional markers that merit work-produce immunity. The firm's agreement with Mandiant characterized the consultant's assistance as "computer security incident response," "digital forensics, log, and malware analysis," and "incident remediation."

Debevoise said in a court declaration that Mandiant had helped the law firm give legal advice by (i) aiding its grasp of "technical matters in documents the firm reviewed and certain witness interviews it conducted;" (ii) "conducting targeted sub-investigations on technical matters related to the incident;" and (iii) performing a "red team exercise to assess

remediation" of the vulnerability that enabled the breach.

The Court concluded that the work resembled what Mandiant would have provided Capital One were the bank immune from lawsuits, and ordered disclosure, citing the law's aversion to blanket evidentiary exclusions that limit truth-seeking.

See "Lessons From SDNY Ruling on How to Preserve Privileged Communications With Attorney Consultants" (Aug. 7, 2019).

Legal Landscape

Second Straight Skeptical Ruling in Virginia Federal Court

The Capital One decision adds to a string of rulings denying privilege for consultants' data breach reports. The Court invoked a December 2019 case, *In re Dominion Dental Services*, that refused to protect a Mandiant post-breach forensic incident report. The Court also cited the *In Re Premera Blue Cross* rulings from Oregon's federal court (2017 and 2019). In *Premera*, as in the Virginia cases, Mandiant had worked for the company before the breach, providing a paper trail. This continuity of relationship colored each court's conclusion that, in total, Mandiant's work did not materially change when outside counsel became involved.

The Virginia and Oregon courts did not address First Amendment issues, though in 2019, a Maryland court ordered Marriott to release a forensic analysis of a large breach it suffered on First Amendment access grounds.

Circuit Split

The *Capital One* order weighed four contrary opinions in other jurisdictions that held that the work-product protection applied to forensic reports addressing data breach incidents experienced by Arby's, Target, Experian and Genesco. The Court discounted some of these precedents, Melodia noted, for being too perfunctory to offer guidance. In contrast, the opinions that the Court relied upon include detailed analyses. "Judges who decide not to provide the protection seem to feel compelled to write more because they are going against the grain," he observed.

Overall, "published decisions and publicly available law still clearly favor protection of forensic reports as work product," Melodia said. When one accounts "for all of the instances when the privilege question has been decided on a conference call, or in a short letter opinion from a magistrate judge, or where it has been on a privilege log and plaintiffs' counsel accepted that without dispute," the argument for granting privilege is even stronger, he contended.

Plaintiffs' attorneys, however, also point to instances where businesses disclosed the reports without published orders. In the Dominion case, plaintiffs' pleadings cited Anthem and Excellus each turning over forensic incident reports without dispute in their data breach class actions.

"We have a variety of opinions now on this topic," noted Paul Luehr, a partner at Faegre Drinker Biddle, and "it's difficult to anticipate how much weight will be put on this particular decision."

One lesson of *Capital One* for companies defending themselves, Melodia offered, is that companies should ask courts that grant protection to forensic reports to write a detailed order explaining their rationales. These courts may not think analysis is necessary, he said, because "they are simply doing what everybody assumes would be done" in extending immunity to such reports.

See "*Target* Privilege Decision Delivers Guidance for Post-Data Breach Internal Investigations" (Nov. 11, 2015).

Preserving Privilege After the *Cap One* Decision

Show the Court More Legal Involvement – Carefully

Courts weighing privilege claims want to know whether "the report was seen and reviewed and revised by counsel. Was it actually done for counsel to be able to give the company legal advice or not?" said Arnold & Porter partner Jami Mills Vibbert, who noted that she could not discuss the Capital One case specifically.

To better satisfy the reviewing court, companies could share details about the lawyers' process around the report. These could include, Melodia suggested, "how often the forensic team checked in with and received direction from the legal team, the framing of the work by the legal team with an eye on legal risks and requirements, and the ways in which the report reflects the joint work product of technical and legal professionals."

Also, lawyers could go beyond the boilerplate in the engagement letter – such as, "the work will be directed by counsel and is intended to help provide legal advice" – to include process expectations and incident specifics.

The downside of discussing process, Melodia said, is that "it could provide a roadmap" for plaintiffs "if anybody involved in the investigation is deposed." The attorneys must not be too effusive, Melodia cautioned. "To put a lot of legal-team fine points into the statement of work or the engagement letter is really risking subject-matter waiver," he explained. Plaintiffs' attorneys will then ask to see "your other documents and your thinking about these five specific legal issues that you've raised," he added.

See "Attorney-Consultant Privilege? Key Considerations for Invoking the *Kovel* Doctrine (Part One of Two)" (Nov. 16, 2016); Part Two (Nov. 30, 2016).

Fold the Forensic Report Into an Appendix

Capital One and the string of decisions before it are stoking fears that lawyers' and forensic investigators' candid conversations could be used against them in court. "If this decision were to be the standard, it discourages a probing forensic analysis of data incidents and committing that work to writing at a most basic level," Melodia said.

Instead, companies and their outside counsel could instead prepare a blended investigative report for the data breach, Vibbert advised. "The best practice is to restrict the forensic material to an appendix for the attorney's investigative report," she suggested.

The appendix would include only the factual findings and details, like log evaluations. With

this approach, the outside counsel folds the rest of the forensic details into the legal advice and discussions in the body of the memo, Vibbert explained.

See "Preserving Privilege Before and After a Cybersecurity Incident (Part One of Two)" (Jun. 17, 2015); Part Two (Jul. 1, 2015).

Ask for In-Camera Review

Whether in an appendix or not, the plaintiffs likely will seek the disclosure of the forensic analysis. Judges in prior cases conducted *in-camera* reviews to evaluate whether a report deserved work-product immunity, Melodia noted. If a judge seems skeptical, defense counsel may ask the judge to review the report to verify the lawyers' handiwork. "That's a better option than receiving an opinion in a vacuum, which maybe makes certain assumptions about the memo that aren't true," he said.

Best Practices Despite the Decision

Don't Wait for a Breach to Hire a Forensic Firm

Among the worst implications of recent decisions like *Capital One*, *Dominion* and *Premera*, Melodia and Luehr agreed, is the preference they seem to afford to companies that hire new forensic experts after the breach. Each decision cited details from the companies' ongoing business relationship with Mandiant as a key factor in their evaluations, Luehr explained. "Then they contrasted that with precedents where the defendants hired teams at the last minute" as clearer scenarios for earning privilege, he added.

This preference for establishing a new forensic relationship post-breach, Luehr cautioned, threatens to undermine a central, best practice in cybersecurity – being ready to respond rapidly. "The GDPR and the New York DFS regulation are pushing companies to report breaches within 72 hours, yet this decision suggests that companies should spend most of that precious time trying to find and sign up a forensic expert at the last minute," he said.

The Court's emphasis, Melodia agreed, "is particularly off base in the financial services industry, where a thorough vetting of vendors is an absolute regulatory requirement through the Fed and OCC and a lot of state banking regulators," he said. "Third-party oversight rules are very demanding. You can't bring just anybody in to start working on the bank's innermost data systems, which contain personal information," he added.

Hiring a new incident response firm post breach is inefficient, risky and costly, Melodia noted. "I've seen investigations held up a week or more at the outset because of contract negotiations or fees," he recalled. During that time, "you are potentially losing evidence, potentially allowing intrusion to continue and potentially delaying engagement with law enforcement," he warned.

Retaining a firm in advance is also prudent, Luehr said, to prepare for a spread of ransomware or times of elevated assaults, as in the current pandemic. Those situations create a run on experienced responders. He recalled instances he has observed "where those who did not make that forensic hiring decision and retention in advance [were] left on the outside looking in," without a trusted consultant.

See "A Roadmap to Preparing for and Managing a Cyber Investigation" (Nov. 14, 2018).

Lawyers Should Keep Setting the Forensic Agenda

The *Capital One* decision is out of step with the prevailing reality of forensic investigations after an incident, Luehr noted. It gives the impression that lawyers and forensics investigators work separately – as if the lawyers unlock the work room, hand over admin passwords, then let the forensic team alone to burrow into the logs and networks.

In practice, "the forensic report that most experts generate is driven almost exclusively by the law," Luehr said. The outside counsel asks the cybersecurity consultants to look for details that clarify whether the company must notify affected individuals, regulators and the markets.

Focusing the forensic investigators may require some pushing, as they intuitively are "interested in how the attackers got in and how you button up that hole. Often, they want to fix the problem and move on," Luehr said. Without a lawyer's urging, "they would not pay attention to PII or what jurisdiction affected people are in," he added.

Vibbert agreed that the law firm must guide the forensic team, for example, to ensure review of a broad enough array of data categories. "It's not the forensic investigator's job to know that certain terms have legal meaning and may be construed as evidence," she said. It is hard to imagine that this decision will lead to lawyers pulling back from working closely with forensic analysts. Without cooperation with forensics, lawyers will be unable to quickly determine the company's obligations and will not be able to properly notify regulators and business partners.

The collaboration of legal and forensics professionals is crucial for evaluating the litigation risk, Luehr said, as they assess the history of the company's defenses and "how far along the company was in its maturity journey to reasonable security." Focal points that merge technical and legal questions, Melodia added, include whether a breached company's staff ignored red flags, lacked a proper protocol, or were using last year's best practices instead of this year's.

See "Answers to Four Critical Questions on Privilege in Internal Investigations" (Dec. 5, 2018).

Keep Collaborating Closely Post Breach

The *Capital One* opinion, Melodia lamented, undercuts the hard-won learning of the past decade about how to best respond to a breach. "It goes back to the day when there were very siloed individual experts after an incident," he said.

"It used to take a long time and a lot of work," for the different professionals to investigate separately, Melodia recalled. The various players had to figure out how to talk to each other, protect the company's different interests, synthesize the risks into a clear picture and eventually decide on a response. The delay hurt both sets of victims – the company and the affected individuals, he noted. "It's taken more than a decade for the clients to understand how the response is a team sport," he recalled.

Debevoise told the Court that it had conducted 160 interviews. Melodia observed that, if the investigation were "as thorough and deep" as

that sounds – cautioning that he had not seen more details – the lawyers likely had shaped the forensic work. Capital One's counsel and the plaintiff's lawyers did not reply to requests for comment about the collaboration, evidence available to the Court and Debevoise's work product.

See our three-part series on protecting attorney-client privilege and attorney work product while cooperating with the government: "Establishing Privilege and Work Product in an Investigation" (Feb. 8, 2017); "Strategies to Minimize Risks During Cooperation" (Feb. 22, 2017); and "Implications for Collateral Litigation" (Mar. 8, 2017).

Is It in the Public's Interest to Expand Privilege?

If we see more decisions like this, Vibbert and Melodia agreed, companies may start to pursue more protection from courts for breach planning and response. A December 2019 report from the Sedona Conference laid out the case for a qualified privilege for cybersecurity information prepared both before and after security events. "You want companies to laser-focus on stopping the bleeding, not to think about the liability that might arise because of the attack," said Vibbert, who helped prepare the report.

"In most companies' incident response plans," Vibbert noted, "the first call is to the lawyers, because of liability issues. But that slows down the provision of information" to law enforcement and regulators, which hurts the overall response.

Companies could start citing this white paper in filings to courts or ask legislatures and courts to extend protection in evidentiary rules, Vibbert said. "Because the attacker is, in many cases unknowable, and the entity on the hook is the victim of the crime, this is a unique circumstance and we could have a public policy of affording more protection when a company finds out about a security incident," she argued. The Cybersecurity Information Sharing Act of 2015 may persuade authorities to consider the idea.

Attorney oversight of every aspect of the forensic investigation and the creation two separate teams is expensive and misplaces priorities, Vibbert added. "The thing companies should not be doing first is trying to protect documents," he said.