Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

It's Getting Harder To Hide Consultants' Data Breach Reports

By **Ben Kochman**

Law360 (June 3, 2020, 10:10 PM EDT) -- Capital One is the latest company ordered by a U.S. court to disclose a consultant's analysis of a massive data breach, in a potential boon for consumers but a troubling development for businesses aiming to talk frankly about breaches without fear of legal repercussions.

In a ruling delivered last week, a Virginia federal magistrate judge rejected Capital One's bid to keep private a report prepared by cybersecurity firm Mandiant analyzing a 2019 breach that the bank says exposed the personal data of more than 100 million people.

Capital One had argued that the report — which could include key details about how accused hacker Paige A. Thompson allegedly made off with the data trove — should be protected by attorney-client privilege because it was commissioned while the bank's lawyers were preparing for an onslaught of litigation stemming from the breach announcement.

U.S. Magistrate Judge John F. Anderson disagreed, **finding that** Capital One, which already had Mandiant on retainer, would have likely ordered the forensic report even if it did not expect legal action.

"The retention of outside counsel does not, by itself, turn a document into work product," the judge wrote.

Last week's opinion has struck a nerve with attorneys who counsel businesses as they respond to data breaches, with lawyers saying the decision, along with similar recent rulings, could chill efforts to respond to cyberattacks in real time given fears that conversations about the breaches could someday be used against companies in court.

"It is important for companies and their counsel to have protected communications so that victims of cybercrime can receive candid and comprehensive legal advice," said attorney Michael Phillips, chief claims officer at the cybersecurity analytics company Arceo.ai.

"The decision by the court is concerning because future plaintiffs' lawyers may use it to weaken this core principle," Phillips told Law360.

But lawyers for consumers and other parties suing businesses in the wake of data breaches argue that they have the right to see the forensic reports, which can provide a rare third-party perspective on how a breach actually happened.

"Any company that keeps the personal information of its customers should perform a post-breach investigation to determine how the breach occurred as a function of its business — not just to obtain legal advice," said plaintiffs attorney Amy Keller of DiCello Levitt Gutzler LLC. Keller is representing consumers suing Marriott in **closely watched litigation** stemming from the hotel giant's November 2018 admission that a data breach exposed the personal details of up to 383 million guests.

"Shrouding those investigations from disclosure based upon work product or attorney-client communications is a disservice to the individuals whose information was exposed," Keller said.

The Capital One ruling is the latest in a string of decisions ordering companies to turn over third-party analyses of data breaches. It comes months after a Maryland federal judge overseeing shareholder litigation over the Marriott breach — the result of a cyberattack on Marriott's Starwood guest reservation database — **ordered the hotel giant** to disclose another form of third-party report that it had attempted to keep private.

The judge said the public had a First Amendment right to view the report, which was produced by forensic analysts Marriott had hired as part of an investigation by payment card issuers after the breach.

And in October 2017, in a case more similar to the Capital One privilege dispute, an Oregon federal judge ordered health care benefits provider Premera Blue Cross to produce a large chunk of the **documents requested** by customers in litigation over a 2015 data breach affecting about 11 million people. Those documents were also prepared by Mandiant, which is now part of the cybersecurity company FireEye.

"There is a trend among judges favoring release of digital forensic reports, despite the legalese-laden efforts by corporate lawyers to keep them confidential," John Reed Stark, a data breach response and digital compliance consultant and senior lecturing fellow at Duke University Law School, told Law360.

It's unlikely that corporate attorneys will start advising clients to simply hand over the third-party forensic reports that some view as a potential road map of liability, however.

Stark said that the Virginia court's ruling in effect incentivizes companies to take onerous measures to try to differentiate post-breach communications from normal communications with cybersecurity consultants, in an effort to claim that those communications are protected by attorney-client privilege.

Based on the court's reasoning, companies that already have forensic analysts on call but that want to preserve privilege could try hiring a new forensic firm just to deal with the breach — a move Stark said "makes little practical sense."

Companies could also try asking their forensic firms to draft a letter to their law firm summarizing their investigations in broad terms rather than getting into specifics like the "precise parameters of the attack vector," or choose to eschew receiving such a report at all, Stark said.

"If a report is not specifically required by contract or law, skip the drafting of a forensic report altogether," Stark suggested.

Phillips agreed that the Virginia court's opinion still "provides a road map to preserving privilege in an investigation," if companies are careful to distinguish data breach investigation reports as a distinct form of communication with their cybersecurity consultants.

"Companies and their security partners should consider creating separate statements of work for breach investigations," Phillips said, adding that "a company's data breach investigation process should look and feel different than typical operations with a managed security provider."

The case is In re: Capital One Customer Data Security Breach Litigation, case number 1:19-md-02915, in the U.S. District Court for the Eastern District of Virginia.

--Editing by Aaron Pelc.
