In In Re Capital One Consumer Data Security Breach Litigation, 2020 WL 2731238 (E.D. Va. May 26, 2020), Magistrate Judge John F. Anderson found that a report prepared by a cybersecurity firm acting under the direction of counsel would have been prepared regardless of any anticipated litigation and accordingly was not protected work product.

In this data breach litigation, plaintiffs sought discovery of a report prepared by a cybersecurity investigation firm related to a data breach. Id at *1. Prior to the data breach, Capital One had entered into a master services agreement with a cybersecurity firm to provide, among other things, incident response services in the event of a data breach. When Capital One experienced the data breach, it retained a law firm to provide legal advice in connection with the breach and directed the cybersecurity firm to perform incident response services at the direction of the law firm. Immediately following the public disclosure of the data breach, several lawsuits, including the instant one, were filed.

The magistrate judge noted that the work product doctrine shields only documents prepared because of the prospect of litigation. Id. at * 3 (italics in original). He explained that "[t]he 'because of standard' is designed to protect only work that was conducted because of the litigation and not work that would have been done in any event." It is not enough to render documents protected work product if they were also created because of the prospect of litigation. In other words, to determine whether documents was created because of anticipated litigation, a "but for" causation test applies. Id. at *4.

As an initial matter, Judge Anderson acknowledged that "there was a very real potential that Capital One would be facing substantial claims following its announcement of the data breach." There was no question that at the time of the breach, Capital One anticipated litigation. The crucial issue, therefore, was whether the cybersecurity firm's report "would have been prepared in substantially similar form but for the prospect of that litigation." The burden of showing that a document would not have been created but for the potential for litigation rests with the party requesting the work product protection.

After examining the circumstances of the cybersecurity firm's retention, Magistrate Judge Anderson concluded that the report the firm generated would have been produced regardless of anticipated litigation. Id. at * 7. Important to Judge Anderson's analysis was that Capital One had entered into the master services agreement with the cybersecurity firm in advance of any data breach. Id. at *4. The master services agreement detailed the incident response services the cybersecurity firm was to provide in the event of a data breach. Capital One sent a letter to the cybersecurity firm at the time of the data breach directing it to perform the same services as had been agreed to in the master services agreement. Although the letter directed that the work be done at the direction of a law firm, the services to be performed were identical. Judge Anderson also observed that at the time Capital One and the cybersecurity firm entered into the master services agreement, the retainer paid was consider a "business-critical expense and not a legal expense."

Also relevant to Judge Anderson's analysis was that Capital One did not offer any statement or evidence that it would not have had the cybersecurity firm generate a substantially similar report absent the prospect of litigation. The fact that the cybersecurity firm performed its work under the direction of a law firm and initially provided its report to the law firm was not enough to show that the report would have been substantially different even absent the prospect of litigation.

Judge Anderson concluded that the cybersecurity firm would have generated a report similar to the one it produced regardless of whether there was a prospect of litigation. The report, therefore, could not be withheld as work product. Id. at * 7. Although Judge Anderson held that the cybersecurity firm's report was not work product, he declined to decide whether material related to the report would also have been produced absent the prospect of litigation and so did not rule whether such material could be protected as work product.