Treat Your Data Breach Investigation Like Your Toothbrush—Don't Share It with Anyone

By Daniel J. DeFiglio

DANIEL J. DEFIGLIO *is a partner at Archer & Greiner, P.C. and a member of its business litigation, trade secret and noncompete, and cybersecurity practice groups.*

No dentists have endorsed this statement. But several district courts—including ones within the Third Circuit—have (at least theoretically). Technology officers and corporate counsel should thus take heed: if you are not careful in responding to a data breach, your well-intentioned data breach investigation report could end up as "Exhibit 1" in later litigation.

This article will explore three recent federal court decisions related to the discoverability of so-called "data breach investigation reports," and offer practical considerations based on those decisions.

Background

New Jersey requires "any business that conducts business in New Jersey" to disclose any "breach of security"—defined as "unauthorized access to electronic files, media or data containing personal information"[1]—"in the most expedient time possible and without unreasonable delay."[2] For purposes of this article, this is what is meant by a "data breach."[3]

Following any data breach, businesses may undertake what is referred to as a data breach investigation. The scope and purpose for conducting a data breach investigation vary depending on the needs of the business. A larger company that handles an immense amount of financial or personal information, for example, may hire a specialized outside vendor to conduct a full-scale forensic examination of its computer environment. Smaller companies may investigate the matter internally (for example, with IT staff), or on a more-limited basis. For purposes of this article, a data breach investigation report refers to any written report that arises out of these investigations.

For many years, the discoverability—*e.g.*, the ability of an adversary to obtain something through discovery in litigation—of these data breach investigation reports was somewhat unsettled. Several cases within the past two years, however, have begun to cement the resolution of this issue. Those cases, discussed more fully below, are *Capital One,*[4] *Clark Hill*,[5] and, recently, *Rutter's*,[6] and provide several considerations for businesses faced with data breaches.

The *Capital One* Decision (May 2020)

The oldest of these cases is *Capital One*, which was decided in May 2020. The factual predicate of *Capital One* is probably familiar to most because it was reported in various nationwide news outlets.[7] As a recap, "in March 2019 a data breach occurred whereby an unauthorized person gained access to certain types of personal information relating to Capital One customers."[8] Relevant here is Capital One's response to that data breach.

According to the District Court opinion, in 2015, Capital One executed a master services agreement (MSA) with a company called FireEye, Inc. d/b/a Mandiant. This MSA was then extended through a series of purchase orders and statements of work (SOW) for several years. In 2019, Capital One paid Mandiant a retainer for a SOW that entitled Capital One to 285 hours of services. The 2019 SOW included services like "computer security incident response; digital forensics, log, and malware analysis;...incident remediation," and, in the event of a breach, a "detailed final report."[9]

After the breach was discovered on or about July 19, 2019, Capital One hired an outside law firm to provide legal advice. The law firm retained Mandiant to "provide services and advice concerning 'computer security incident response; digital forensics, log, and malware analysis; and incident remediation;'" in other words, the same services Mandiant was already providing under the 2019 SOW. According to the law firm's agreement with Mandiant, Mandiant was to be paid in accordance with the terms of the MSA and 2019 SOW, but was to work at the direction of the outside law firm.

Following its investigation, Mandiant issued a report to the law firm detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security. The law firm provided a copy of the Mandiant Report to Capital One's legal department, its board of directors, approximately 51 Capital One employees, four regulators (e.g. Federal Deposit Insurance Corporation, Federal Reserve Board, Consumer Financial Protection Bureau, and Office of the Comptroller of the Currency), and an outside accounting firm.

Despite acknowledging that litigation was foreseeable when Mandiant began its investigation (the first lawsuit was filed days after Capital One's public announcement of the breach),[10] the Court found that the Mandiant report was not privileged. In the Court's view, the determinative issue was whether the Mandiant Report "would have been prepared in substantially similar form but for the prospect of that litigation.""[11]

The Court relied on at least three facts in finding the answer to this question was "yes" (meaning the report was not privileged). First, "Capital One had a long-standing relationship with Mandiant and had a pre-existing SOW with Mandiant to perform essentially the same services that were performed in preparing" the Mandiant Report.[12] Second, Mandiant was paid for its initial work under the Letter Agreement out of the retainer already provided to Mandiant under the 2019 SOW between Mandiant and Capital One.[13] And third, Capital One's disclosure of the Mandiant Report to outside regulators and an outside accounting firm—while not explicitly a waiver—was evidence that its investigation was "significant for regulatory and business reasons," as opposed to in anticipation of litigation.[14] Thus, the Court found that the Mandiant Report would have been prepared in a substantially similar form even if there were no prospect of litigation. Thus, it was not privileged.

The *Clark Hill* Decision (January 2021)

Clark Hill applied similar logic, but went a step further. In *Clark Hill*, the defendant claimed that it had conducted a "two-tracked investigation," wherein its "usual cybersecurity vendor, called eSentire" investigated the data breach to preserve "business continuity;" a separate cybersecurity vendor (Duff & Phelps) conducted a second investigation for the "sole purpose of assisting [the outside law firm] in gathering information necessary to render timely legal advice."[15]

While the Court did not appear to disagree with the two-tracked premise, it found that the defendant's "two track story finds little support in the record:" meaning *Clark Hill* could not carry its

burden to show that the Duff & Phelps report was privileged. Of central importance to the Court's reasoning was: (1) there was "no evidence that eSentire ever produced any findings, let alone a comprehensive report like the one produced by Duff & Phelps;"[16] (2) the Duff & Phelps report was "shared not just with outside and in-house counsel, but also with "select members of Clark Hill's leadership and IT team," and, later, the FBI;[17] and (3) the defendant certified that it had used the report to manage "any issues . . . related to the cyber incident."[18] Basically, the *Clark Hill* court found that although the defendant had "papered the arrangement using its attorneys," the facts showed that Duff & Phelps' involvement (and, later, its report) had a much broader role than merely assisting outside counsel in preparation for litigation." Thus, the report was not privileged and had to be produced.[19]

The *Rutter's* Decision (July 2021)

Rutter's[20] reached the same conclusion, but for different reasons. There, Rutter's—a chain of gas stations and convenience stores—experienced a cybersecurity event on or about May 29, 2019. On the same day, Rutter's hired an outside law firm "to advise Rutter's on any potential notification obligations."[21] The law firm then hired a third-party cybersecurity consultant—Kroll Cyber Security, LLC — "to conduct forensic analyses on Rutter's card environment and determine the character and scope of the incident."[22] From there, Kroll gathered and analyzed "pertinent facts," including forensic images and "virtual machine snapshots of a sample of potentially affected in-store site controllers."

In total, Kroll's investigation took approximately two months, concluded in July 2019, and included a written data breach investigation report that later became the subject of a discovery dispute.[23] As in *Capital One* and *Clark Hill*, Rutter's asserted the report was protected by both the work product and attorney-client privileges. In determining that neither privilege applied, however, the Court relied on two key facts. First, the Court observed that Kroll's SOW "demonstrates that Defendant did not have a unilateral belief that litigation would result at the time it requested the Kroll Report."[24] Indeed, according to the Court, "[w]ithout knowing whether or not a data breach had occurred, Defendant cannot be said to have unilaterally believed that litigation *would* result."[25] Second, Rutter's corporate designee apparently testified that "Kroll would have prepared—done this work and prepared its incident response investigation regardless of whether or not lawsuits were filed six months later[.]"[26]

Practical Considerations

While every company will have different challenges and concerns in the event of a data breach, the above cases illustrate several considerations for C-suite level management and corporate counsel when conducting data breach investigations. Thematically, though, the primary consideration should be differentiation, *e.g.* how will the company show that the data breach investigation it seeks to protect was "different" than what it would have otherwise done.

Extrapolating from these cases, some factors to consider are:

1. Retaining outside counsel and experts specifically for the investigation you wish to shield; while this is not a determinative factor, *see, e.g.*, *Capital One*, it can aid in this process of differentiation.
2. Clarifying the purpose of any SOWs to address specific legal issues that may arise in litigation, as opposed to merely assessing compliance with laws and regulations. This was a primary issue in *Capital One* and *Rutter's* and underscores the value of close collaboration between outside law firms and cybersecurity vendors in the early stages of a data breach response;
3. Using and describing techniques used in the investigation in the statement of work, and making sure that they are not the same as those used in assessing compliance with federal and state laws. As noted, that the 2019 SOW and Letter Agreement in *Capital One* described nearly identical services was an important consideration in the Court's ruling;
4. Treating each step of the investigation

as if it is work product from the beginning, and not merely "papering the file" as the Court observed in *Clark Hill*; and, finally

5. Not sharing the report outside the litigation control group. This was a factor in all three cases (hence, the title), wherein the breach investigation report was shared with, among others, outside regulators,[27] members of the company's IT team,[28] and the FBI.

The above list is by no means exhaustive; there are certainly other things businesses could do that are not mentioned. Nor does following these steps ensure that a data breach investigation report will not be discoverable. Nevertheless, the lessons of these cases provide valuable insights that businesses may want to consider to protect their investigative reports.

Conclusion

Data breach investigations are valuable tools for businesses that have experienced a data breach. They can provide valuable insights to help better protect customer privacy, and can assist in responding to governmental authorities and private litigants. Yet the cases discussed herein highlight that these same advantages may also be a reason why well-intentioned reports may later become "Exhibit-1" at trial; namely, that the report was made to serve business purposes, not as a defense to litigation. Businesses must therefore be mindful of how these reports are created and shared so that they can obtain the full panoply of their benefits. ■

Endnotes

1. N.J.S.A. 56:8-161.
2. N.J.S.A. 56:8-163.
3. Because there is currently no federal data breach law, states are free to, and have, adopted a patchwork of statutes that define the term differently. This article will not endeavor to explain the differences among the states.
4. For example, Capital One. *See In re Cap. One Consumer Data Sec. Breach Litig.*, No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238, at *1 (E.D. Va. May 26, 2020), *aff'd,* 2020 WL 3470261 (E.D. Va. June 25, 2020).
5. *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 12 (D.D.C. 2021).
6. *In re Rutter's Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 WL 3733137, at *1 (M.D. Pa. July 22, 2021).
7. nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
8. *In re Cap. One,* No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238, at *1.
9. *Id.*
10. *Id.* at *4 ("There is no question that at the time Mandiant began its "incident response services" in July 2019, there was a very real potential that Capital One would be facing substantial claims following its announcement of the data breach")
11. *Id.*
12. *Id.*
13. *Id.* at *2.
14. *Id.* at *4.
15. *Clark Hill, PLC,* 338 F.R.D. at 11.
16. *Id.*
17. *Id. at* 12.
18. *Id.*
19. The court also found that the report was not privileged as an attorney-client communication the Duff & Phelps report (which it reviewed) was used to gain Duff & Phelps's expertise in cybersecurity, not in obtaining legal advice from its lawyer. *Id.* at 13.
20. *In re Rutter's,* No. 1:20-CV-382, 2021 WL 3733137, at *1.
21. *Id.*
22. *Id.*
23. *Id.*
24. *Id.* at *2. Kroll's SOW apparently described its services as an investigation "to determine whether unauthorized activity within the Rutter's systems environment resulted in the compromise of sensitive data, and to determine the scope of such a compromise if it occurred." *Id.*
25. *Id.*
26. *Id.* Applying reasoning similar to *Clark Hill*, the Court also found that Kroll's report was not subject to the attorney-client privilege because it discussed "facts," not "opinions" or "tactics." *Id.* at *3.
27. *In re Cap. One*, No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238, at *2.
28. *Clark Hill, PLC*, 338 F.R.D. at 12 ("select members of Clark Hill's leadership and IT team"); *see also In re Rutter's,* No. 1:20-CV-382, 2021 WL 3733137, at *3 (explaining the report was shared with Rutter's IT personnel).