TRAUB LIEBERMAN

CYBER LAW BLOG

August 10, 2021

Pennsylvania District Court Rejects "Work Product" Protection for Forensic Report Prepared After Data Breach

BY: Jason Taylor

When a data breach occurs, the affected company (or preferably its counsel) will retain a data security or forensics firm to investigate the breach and prepare a report. Forensic reports of a data breach typically identify the likely method by which the hacker accessed a company's data, exposing critical vulnerabilities in its systems. The forensic report may also identify areas in which a company failed to maintain industry standards or to maintain its contractual or other obligations to protect clients and employees' information. When properly prepared, these reports are privileged from disclosure in subsequent litigation based on protections afforded by the "work product" doctrine or similar privileges. However, such privileges are not absolute. Recently, in *In re Rutter's Data Security Breach Litigation*, Case No. 1:20-CV-382 (M.D. Penn. July 22, 2021), a Pennsylvania District Court ordered production of an investigative report created after the defendant was notified of a potential data breach, rejecting defendant's arguments that the report was protected by the work product doctrine and the attorney-client privilege.

In May 2019, Rutter's received two alerts on its data security system which "detail[ed] the execution of suspicious scripts and indications of the use of potentially compromised credentials." That same day, defendant hired outside counsel, BakerHostetler, who then hired a third-party cybersecurity consultant, Kroll Cyber Security "to conduct forensic analyses on Rutter's card environment and determine the character and scope of the incident." Kroll created a report which captured "forensic images" and "virtual machine snapshots of a sample of potentially affected in-store site controllers." At the time, defendant and BakerHostetler understood Kroll's work to be privileged work product. Plaintiffs later filed a class action lawsuit seeking damages arising from the data breach.

In the litigation, plaintiffs sought production of the Kroll Report and related communications between Kroll and the defendant. The defendant company argued that the report prepared by Kroll after defendant was alerted of possible fraudulent activity was protected from discovery by the work product doctrine, which generally serves to protect documents prepared by or on behalf of attorneys in anticipation of litigation. A document is prepared in anticipation of litigation if "in light of the nature of the document and the factual situation of the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation." Moreover, aiding in "identifiable" or "impending" litigation must have been the "primary motivating purpose behind the creation of the document." According to the District Court, to determine whether the anticipation of litigation is the actual purpose behind the report, the initial inquiry is into whether the party that ordered or prepared the document had a "unilateral belief" that litigation would result. Second, the anticipation of litigation must be objectively reasonable.

© Traub Lieberman Straus & Shrewsberry LLP

The District Court found that these two inquiries did not support defendant's work product claim. According to the court, the contract between Kroll and the defendant made it clear that the primary motivating purpose behind the Kroll Report was not to prepare for the prospect of litigation. For example, the contract included a "statement of work" (SOW) and a description of services providing that "[t]he overall purpose of this investigation will be 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." This language, according to the court, demonstrated that the company did not anticipate litigation at the time that it requested the Kroll Report, but rather to determine whether sensitive data was compromised. Because the purpose of the report was to determine *whether* a breach occurred, and the scope of such breach, the company could not have unilaterally believed that litigation would certainly result. Additionally, at defendant's corporate deposition, its corporate designee testified that litigation was not contemplated at the time the Kroll Report was prepared, further undermining its anticipation of litigation arguments.

The District Court also held that the Kroll Report was not protected by the attorney-client privilege. The privilege applies to communications between a client and its attorney when discussing legal strategies and tactics. The court found that the Kroll Report was factual in nature, which is not protected by the attorney-client privilege. The Kroll Report reported data collected from defendant's equipment and had the purpose of determining whether the equipment was compromised and to what extent. The District Court determined that this was purely factual, and not legal strategy. Similarly, Kroll's role in the investigation was not legal assistance because they are not professionals in the field of law. Moreover, the report was provided to defendant when it was completed and not BakerHostetler. Kroll worked alongside defendant's IT personnel to identify and remediate potential vulnerabilities, and not defendant's attorneys. Accordingly, Kroll's services were not deemed to be "gaining or providing legal assistance," as neither Kroll nor Rutter's IT personnel were professionals in the field of law and the services involved those two entities working alongside each other with no mention of attorney involvement.

Ultimately, the court found that the defendant had not presented sufficient evidence to show that the report was protected under any work-product or attorney-client privilege, and thus granted Plaintiff's motion to compel production of the Kroll Report. Absent clear intention of a "unilateral belief" of impending litigation, such reports and others like it are not protected by the work product privilege. While the decision is another reminder of the difficulties large companies have in protecting their investigation of data breach events, the court's analysis does provide some lessons for companies and counsel in how to ensure that forensic reports remain protected. Namely, retain counsel early and ensure that counsel has an active, rather than passive role in the investigation. The company and counsel should also understand that in this day and age litigation is likely after a data breach and they should prepare accordingly. Counsel and the company should limit disclosure of any forensic report to the companies legal team only where possible, and ensure that preparation of any documents or reports are for purposes of litigation only.

© Traub Lieberman Straus & Shrewsberry LLP