April 2018

Mendes Insights

Breach Response and Preserving Privilege

When are forensic vendor documents covered by "privilege?"

Cyber/Data Privacy and Security

In a recent decision out of the United States District Court in Oregon, the Court entered a ruling that has implications for breach responders everywhere.[1] *While many professional experts and outsourced vendors routinely retained in a litigation context are well-versed in how to communicate via counsel, there are certain scenarios involving the urgency in responding to a potential data breach that have challenged the usual best practices for parties involved. Is it better to have a separate entity come in post-breach to perform the same analytics as your usual security firm? What can in-house counsel do to maintain privileges once aware of an incident? Does it make a difference how documents are labeled or how reports are titled? While some judicial findings may raise more questions than answers, the decisions highlight important practical considerations for entities in response-and-remediate mode.*

Premera Ruling

Breach

In March of 2015, Premera Blue Cross, a not-for-profit Blue Cross Blue Shield licensed health plan provider based out of Washington State, issued a press release stating that it had been the victim of a data breach. Premera disclosed that there were potentially 11 million victims, that the breach was discovered in January 2015 but took place eight months earlier, and that the data impacted included medical and financial information of current and former customers.[2] Premera also announced that it was working with an outside security firm, Mandiant, as well as the FBI, in order to investigate the attack.

Class Litigation

Over thirty class actions were filed against Premera, which were eventually consolidated before one federal court judge, Hon. Michael H. Simon, in the U.S. District Court for the District of Oregon.[3] Plaintiffs alleged violations of various state consumer and breach disclosure laws, as well as negligence, breach of contract and misrepresentation by omission, amongst others, and survived Premera's motion to dismiss, including a defense that their claims were preempted by federal laws.[4] As a result, the parties proceeded with the discovery phase of the case.

Attorney-Client Privilege and Work-Product Doctrine

Investigation of a Breach

In discovery, Plaintiffs sought documents relating to work performed by Defendant's third-party vendor, Mandiant, as well as documents relating to work performed by additional third-parties, like Defendant's public relations firm and other technical vendors, including the e-discovery consultants.[5] Premera objected on the basis that the documents were protected by attorney-client privilege or attorney work-product doctrine. Plaintiffs specifically sought production of Mandiant reports and potentially drafts of reports. The Court noted that Mandiant was hired by Premera in October 2014 to review its data management system and then, as of January, Mandiant discovered the existence of malware. Thereafter, by February of 2015, in light of the discovery of this data breach, Premera hired outside counsel, which was reportedly in anticipation of litigation. The day after counsel was hired, Mandiant and Premera entered into an amended statement of work that shifted supervision of Mandiant's work to outside counsel. The Court noted, however, that the scope of work did not change from the earlier agreement entered into as of October 2014.[6]

The Court was not persuaded that Mandiant's work was privileged and protected as work-product. The Court found that the only change in the scope of work to be performed by Mandiant was that it was subsequently "directed to report directly to outside counsel and to label all of [its] communications as 'privileged,' 'work-product,' or 'at the request of counsel.'" The Court stated that Premera's argument that Mandiant's role "became more like that of an investigator" was not supported by the amended statement of work.[7]

The Court contrasted the Premera breach scenario with the situation in another federal data breach case involving the retail giant Target.[8] In that case, the company performed its own "independent data breach investigation that was produced in discovery and the attorneys performed a separate investigation through a retained expert company that was privileged and protected from discovery."[9] The Court also distinguished the Premera case from the facts in a data breach case filed against the credit monitoring company Experian, which coincidentally also involved

Mandiant.[10] The Premera Court noted that in the Experian case, Mandiant was hired by the outside counsel that had been engaged by Experian, whereas Mandiant was already working under Premera's supervision before outside counsel became involved.

Significantly for practitioners, the Court found that "Premera has the burden of showing that Mandiant changed the nature of its investigation at the instruction of outside counsel and that Mandiant's scope of work and purpose became different in anticipation of litigation versus the business purpose Mandiant was performing when it was engaged by Premera before the involvement of outside counsel."[11] With respect to the "work-product" protection, the Court looked at the "dual-purpose" test and found that given the "totality of the circumstances," there was no evidence that Mandiant changed its scope or purpose at the direction of counsel. However, given Mandiant's role in working with outside counsel, the Court found that if there are specific documents or portions of documents that contained privileged information[12] or work product information[13], such documents may be withheld by Premera.

Litigation-Related Activities

With respect to the other vendors, the Court was somewhat more tolerant of claiming privileges for those vendors retained only by outside counsel. Notably, another typical response vendor, Epiq, was found by the court to have created documents "that are or may be related to legal functions" and thus properly protected (really, the Court resolves this issue much more succinctly than how it addressed Mandiant). With respect to the e-discovery vendors, the Court begins by saying that "it is unclear whether the work performed is of a legal or business nature." Ultimately, the Court notes (with the rare judicial use of a double-negative) that the services performed by the e-discovery vendors "would not constitute non-legal business functions" and thus those documents may be protected as privileged or work-product.[14]

Practical Implications

Entities are faced with some daunting challenges when attempting to tackle the repercussions of a data security breach. The clock is ticking to stop intruders, preserve data, remediate any losses and then comply with relevant regulations and their own privacy or security policies. The inclination to retain, or keep on hand, the security firm that can quickly and knowledgeably restore your systems is a commendable one. As revealed in the cases discussed above, some of the largest and most sophisticated data handlers have struggled to reconcile the tensions created by the need to rapidly respond to a breach while maintaining appropriate privileges and defenses. However, the cases also illustrate that certain practices have a greater chance of surviving challenges. Once unauthorized access is identified: retain counsel; have outside counsel retain the forensic firm;

prepare documents and communications in anticipation of litigation, for purposes of preparing for litigation. Some of these practices are tried and true, but in the immediate aftermath of an entity-wide disruptive event, even the most diligent can be at risk of overlooking this critical chronology. As they say, timing is everything.

---

[1] *See, In Re: Premera Blue Cross Customer Data Security Breach Litigation*, No: 3:15-md-2633-SI, 2017 U.S. Dist. LEXIS 178762, ---F.Supp.3d___ (D. Or. Oct. 27, 2017).
[2] https://www.seattletimes.com/business/premera-sued-over-security-breaches/ ; https://www.forbes.com/sites/katevinton/2015/03/17/11-million-customers-medical-and-financial-data-may-have-been-exposed-in-premera-blue-cross-breach/#42766a3375d9
[3] https://www.bizjournals.com/seattle/blog/techflash/2016/01/after-premera-breach-new-washington-cybersecurity.html
[4] https://www.lexislegalnews.com/articles/14797/data-breach-class-claims-against-premera-mostly-survive-dismissal-motion
[5] Plaintiffs also sought documents withheld by Premera based on "joint defense" or "common interest" privileges; and documents that Premera asserted incorporated advice of counsel or prepared at the request of counsel. *See Premera* at *3.
[6] *Id.* at *7.
[7] *Id.*
[8] *See, In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 WL 6777384 (D. Minn Oct. 23, 2015).
[9] *Premera* at *7.
[10] *See, In Re Experian Data Breach Litig.*, Case No. 8:15-cv-01592-AG-DFM (C.D. Cal. May 18, 2017)
[11] *Id.* at *8.
[12] Documents prepared for the purpose of communicating with an attorney for the provision of legal advice.
[13] Documents which contain the mental impressions of counsel; communications to counsel to provide facts to prepare for litigation; or, involve investigation solely at the behest of counsel.
[14] *Id.* The Court earlier addresses public relations firms – finding that their services were a "business function," even though retained by counsel, and thus not protected by a privilege. *See Premera* at *5.