PUBLICATION

Protecting Breach Investigation Reports in Litigation – Key Actions

June 07, 2017

A recent opinion from the District Court for the Central District of California in *In re Experian Data Breach Litigation* offers some examples of best practices for establishing the work-product privilege over certain investigation reports generated after a breach incident.

The Court's Decision

In September 2015, Experian learned that it had been hacked and that the social security numbers of approximately 15 million of its customers had been compromised. Experian immediately retained outside counsel for legal advice in connection with the breach. Counsel then hired a cybersecurity consultant to educate counsel on the technical issues with the breach and help counsel provide legal advice to Experian. To conduct its work, the consultant reviewed forensic copies of Experian's server and network. It did not have access to Experian's live network.

On October 1, 2015, Experian publicly announced the breach. The first lawsuit against Experian was filed the next day. By the end of October 2015, the consultant finished its investigation of the breach and submitted a report to outside counsel. Outside counsel then shared the report with the in-house lawyers for Experian who in turn discussed the report with the company's board of directors to devise the company's strategy for defending against litigation. Notably, the full report was not given to Experian's incident response team.

In the pending litigation, plaintiff filed a motion to compel production of the consultant's report and documents related to that investigation. Experian opposed the motion, arguing the work-product doctrine shielded the documents because the consultant's work was done "in anticipation of litigation."

On May 18, 2017, the district court sided with Experian and denied plaintiff's motion to compel. The court concluded that Experian established that the company's outside counsel hired the consultant in anticipation of litigation. The court further held:

[t]he evidence here establish[es] that [outside counsel] instructed [the consultant] to do the investigation and, but for the anticipated litigation, the report wouldn't have been prepared in substantially the same form or with the same content.

Moreover, Experian's conclusion that litigation would follow was reasonable since a lawsuit was filed the day after Experian announced the breach. What the court also found compelling was the fact that the full report was not shared with Experian's incident response team. The court, however, cautioned that not all reports prepared by the consultant for Experian were shielded. Since the consultant had provided similar forensic work to Experian in the past, reports submitted to Experian before outside counsel was hired may be subject to production in the lawsuit.

How Can You Protect Your Reports in Litigation?

The court's decision is significant as it offers guidance for shielding the reports of experts hired to assist after breach incidents. However, the court was careful in limiting the scope of its holding to confirm that the application of the privilege must be evaluated on a case-by-case basis.

Based on the *Experian* court's opinion, here are some things to remember for future engagements with counsel and data security experts:

Insist that your legal counsel engage consultants after a breach. Whether the work-product privilege applies is decided by the particular facts of a case. However, the privilege is less likely to apply if a member of your company's operations team engages the expert. The best practice is to engage your experienced outside counsel immediately and allow counsel to engage the consultants. Alternatively, if your company has in-house counsel, allow those lawyers to hire the consultant. Convincing a court that the work-product privilege applies will be easier if you can show that counsel directed the consultant's work.

Clearly identify your company's goals for engaging an expert. If the consultant is needed to help your IT department identify and plug the breach, it is less likely the consultant's findings will be privileged. Under those circumstances, the consultant will need to work with your IT department and incident response team. The privilege may not attach once the consultant's conclusions are widely used in the company's operations.

However, that may not necessarily be a bad thing. Fixing the breach should be priority number one after an incident, and if your internal IT department or incident response team lacks the resources or skill to remediate the breach, hiring an outside consultant will be necessary. Though litigation strategy is important, it does not necessarily need to drive every decision that is made after a breach.

Remember the privilege can be waived. Some breaches trigger a duty to report to a government agency. For instance, HIPAA requires health care providers to report certain breaches to the Department of Health and Human Services. The reporting can lead to an investigation by the Office for Civil Rights. Outside consultants can help with ensuring that the risk that led to the breach is corrected. A report from such experts can also prove helpful in defending yourself during a government investigation. However, the downside is that any potential work-product privilege may be waived once a consultant's report is given to a third-party, like the government.

Be mindful that not all breaches will lead to litigation. To prove that the work-product privilege applies, there has to be evidence that you had an "objectively reasonable" belief that litigation would come from the breach. In the *Experian* case, it was not a stretch for the court to conclude that it was objectively reasonable for Experian to expect a lawsuit from the breach. Given the current litigation climate, companies like Experian are regularly sued when word gets out that sensitive customer information has been compromised. For Experian, it took only 24 hours for the first lawsuit to be filed. However, some types of breaches are not as likely to be litigated. Moreover, the more time that passes between when the breach is made public and the filing of litigation can weigh against a finding of privilege.

Conclusion. As Baker Donelson has noted in prior alerts, we strongly suggest that experienced counsel and forensic investigators are identified prior to the security incident. Knowing your cyber coverage and team will be helpful in the case of an actual incident. See also: https://www.bakerdonelson.com/what-you-need-to-do-now-responding-to-the-major-cybersecurity-attack-against-organizations.

Baker Donelson's Data Protection, Privacy and Cybersecurity Group was recently recognized as a member of the "Honor Roll of Cybersecurity Law Firms" in the United States as determined by The BTI Consulting Group. Recognition as a member of the Honor Roll reflects corporate counsel's view of the Baker Donelson team as strong cybersecurity performers.

If you have any questions about the topics in this Alert, please contact any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Group.