MARCH 08, 2024

Court Applies Work Product Protection to Breach Investigation Reports

One of the most significant questions in data security law is whether reports created by forensic firms investigating data breaches at the direction of counsel are protected from discovery in civil class action lawsuits. They are, at least according to an order issued last week in *In re Experian Data Breach Litigation*. 15-01592 (C.D. Cal. May 18, 2017). This alert analyzes the decision, identifies important practical takeaways for counsel, and places it in context with the two other cases that have addressed this issue.

Why Do Lawyers Hire Forensic Firms?

When a breach occurs, companies often retain legal counsel to advise them on legal issues like whether the company adopted "reasonable" security safeguards; whether the company is obligated to notify affected customers and, if so, when and how; whether notice to regulators is required; and what remedial measures are required. To properly advise clients on these issues, legal counsel needs to know whether personally identifiable information (PII) was affected by the incident, when the intrusion occurred, whether the PII was actually accessed or acquired, what safeguards were in place to prevent the attack, and how the vulnerability was remediated. A good forensic firm will help you answer these questions so you can advise clients accurately.

The reports often contain information that plaintiffs' lawyers would love to get their hands on—they can provide details about why the breach occurred, how it could have been prevented, and whether the company's safeguards were consistent with standards of reasonableness. It is important that the forensic firm be able to

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
305.358.5171
asaikali@shb.com

perform its investigation without fear that its reports will be subject to misinterpretation and criticism by a plaintiff's lawyer or other third party—hence the need for protection of these reports in civil litigation. For the time being, there is no statutory protection for these types of documents (though there should be) so we must turn to the attorney-client privilege and work-product doctrines for protection.

What Happened In *Experian*?

In October 2015, Experian announced that it suffered a data breach, and a class action was filed the next day. Experian immediately hired legal counsel, who in turn hired Mandiant, one of the world's leading forensic firms, to investigate the data breach and identify facts that would allow outside counsel to provide legal advice to Experian.

The plaintiffs requested a copy of Mandiant's report and documents related to that investigation. Experian objected, arguing that the documents are privileged and protected by the work-product doctrine because they were prepared in anticipation of litigation for the purpose of allowing counsel to advise Experian on its legal obligations. The plaintiffs moved to compel production of the documents.

The court held that the documents were protected from discovery by the work-product doctrine. The plaintiffs had argued that Experian had an independent business obligation to investigate the data breach, and it hired Mandiant to do that after realizing its own experts lacked sufficient resources. The court rejected this argument because Mandiant conducted the investigation and prepared the report for outside counsel in anticipation of litigation, "even if that wasn't Mandiant's only purpose." The court pointed to, among other things, the fact that Mandiant's full report was not provided to Experian's internal incident response team. (NOTE: Experian's opposition brief makes clear that Mandiant's report was not shared with the "full" incident response team, so it appears to have been shared with some team members. The information security employee responsible for implementing the remedial measures never saw the report. Additionally, the report was shared with Experian's board of directors to allow in-house counsel to advise the board on legal issues. In other words, the key factor appears to be that the control group was limited.)

The plaintiffs argued that the report should not be protected because it was prepared in the ordinary course of business, citing the fact that Mandiant had previously worked for Experian. The court disagreed because Mandiant's previous work for Experian was separate from the work it did for Experian regarding the subject breach.

The plaintiffs further argued that even if the documents were created to allow counsel to advise Experian, the plaintiffs were not able to obtain the information that was included in the Mandiant report by other means because Mandiant accessed Experian's live servers to do its analysis, which the plaintiffs' experts would not be able to do. The court disagreed, citing information in the record demonstrating that Mandiant never in fact accessed the live servers, but only observed server images to create its report.

Lastly, the plaintiffs argued that even if the information was protected by the work-product doctrine, Experian waived the protection by sharing the documents with a co-defendant (T-Mobile's counsel). In what I believe will be the most underrated yet arguably most important part of the order, the court ruled that the sharing of the report with the co-defendant pursuant to a joint defense agreement did not constitute a waiver of the work-product doctrine.

There are some limitations to the court's order. For example, the court only ruled on whether the work-product doctrine applied to the Mandiant documents, not whether the attorney-client privilege applied. Additionally, Mandiant delivered its report to outside counsel only, who shared the reports with in-house counsel. The full report was not shared with Experian's incident response team (it is not clear who comprised that team). Moreover, Mandiant performed an analysis of Experian's systems two years before this incident. The court did not conclude that the 2013 report was privileged. The court also did not conclude that any work Mandiant performed before outside counsel was hired is privileged. It is not clear from the order whether the court was ruling that the pre-incident and pre-engagement materials were not protected at all, not protected by the attorney-client privilege, or simply not ruling one way or the other. My interpretation is that it is the latter.

How Have Other Courts Ruled?

Only two other courts have addressed the applicability of privilege or work-product protection to the production of forensic reports. Both have applied privilege and/or work product to the documents.

In *In re: Target Corporation Customer Data Security Breach Litigation*, No. 14-2522 (D. Minn. Oct. 23, 2015), the court held that documents relating to a forensic investigation performed to provide legal advice to the company was privileged and work product. Following its breach, Target established a data breach task force at the request of Target's in-house lawyers and its retained outside counsel so that the task force could educate Target's attorneys about aspects of the breach and counsel could

provide Target with informed legal advice. What makes the *Target* case different from *Experian* is that Target undertook ***two*** forensic investigations (both by the forensic firm, Verizon)—one as described (to enable counsel to advise Target in anticipation of litigation and regulatory inquiries) and a second required by several credit card brands (commonly referred to as a "PFI" or payment card forensic investigation). This second investigation, Target conceded, was not protected by privilege or the work-product doctrine. The court allowed production of certain information (emails to Target's Board of Directors, which updated the board on Target's business-related interests), but held that information relating to Verizon's investigation for the data breach task force was protected by the attorney-client privilege and work-product doctrine. The court reasoned that there were forensic images and the PFI documents that the plaintiffs could use to learn how the data breach occurred and how Target responded.

In *Genesco, Inc. v. Visa U.S.A., Inc.*, No. 3:13-cv-00202 (M.D. Tenn. Mar. 25, 2015), the court denied Visa's request for discovery related to remediation measures performed by IBM on Genesco's behalf. The court reasoned that Genesco retained IBM to provide consulting and technical services to assist counsel in rendering legal advice to Genesco. Therefore, the documents were privileged.

Experian came out the same way as *Target* and *Genesco*, but there are subtle differences that should be kept in mind whenever a company decides to retain a forensic company and expects privilege or work product to apply. *Experian* is arguably the most important of the three because it is the far more common scenario. Most companies will not spend money to hire two forensic firms (or one firm with two teams) to perform two separate investigations on the same incident. So where only one investigation is performed, the company and counsel would be wise to read the *Experian* filings and order before commencing the engagement of counsel and a forensic firm.

Takeaways

Here are some practical takeaways if a breached entity wants to minimize the risk of disclosure of a forensic report:

- The forensic firm should be hired by outside counsel, not by the incident response team or the information security department.
- Hire outside counsel early—the work a forensic firm undertakes before outside counsel is involved will not be protected, so the breached entity should engage counsel immediately.

- Create a record and think about privilege issues early in the engagement by doing the following:
    - ensure that the engagement letter between the breached entity and outside counsel envisions that outside counsel may need to retain a forensic firm to help counsel provide legal advice;
    - ensure the MSA and/or SOW between outside counsel and the forensic firm makes clear that the forensic firm is being hired for the purpose of helping counsel provide legal advice to the client;
    - limit the scope of the forensic firm's work to those issues relevant to and necessary for counsel to render legal advice;
    - ensure that the forensic firm communicates directly (and only) with counsel in a secure and confidential manner;
    - limit the group of individuals with whom the report is shared; and
    - incorporate the forensic firm's report into a written legal memorandum to demonstrate how the forensic firm's findings were used to help counsel provide legal advice to the client.

- Sharing a forensic report with legal counsel for a co-defendant in the same data breach lawsuit may not waive the privilege or work-product protection.

In short, preserving the attorney-client privilege and work-product doctrine requires proper planning and knowledge of the traps that could result in waiver. Companies should consult legal counsel now to prepare a protocol they can use when a data incident occurs.