# DATA BREACHES AND THE SIGNIFICANCE OF OUTSIDE COUNSEL

*Privacy, Data Breach & Cybersecurity alert*
May 25, 2017

On May 18, 2017, the Central District of California joined two other district courts (D. Minn. and M.D. Tenn.) in holding that forensic reports resulting from a data breach investigation, conducted at the direction of counsel, are protected from discovery in a civil action, in the case titled *In re Experian Data Breach Litigation*, 15-cv-01592-AG-DFM (C.D. Cal. May 18, 2017). By way of background, in September 2015, Experian learned that one of its systems was breached by an unauthorized third-party. Experian immediately retained outside counsel for legal advice regarding the attack. Outside counsel then hired Mandiant to conduct a forensic investigation and prepare an expert report on its findings. On October 1, 2015, Experian announced the data breach and one day later a class action suit was filed against Experian. Meanwhile, Mandiant finished its report by the end of October 2015 and provided it to Experian's outside counsel. Outside counsel then shared the report with Experian's in-house counsel, but not Experian's internal incident response team.

During discovery, plaintiffs sought production of the forensic report and Experian objected asserting the work-product doctrine. Plaintiffs moved to compel and the Court held that the forensic investigation and report were indeed protected by the work-product doctrine. Specifically, the Court explained that Mandiant's investigation and preparation of its report was not only performed for Experian's outside counsel "in anticipation of litigation," but it was used by Experian's outside counsel to develop its legal strategy. The Court noted that upon completion of the full report, Mandiant provided the report to outside counsel, who shared the report with Experian's in-house counsel, but ***did not share*** the report with Experian's internal incident response team. This is significant when you juxtapose the Experian holding with the holding in *In re: Target Corporation Customer Data Security Breach Litigation*, 2015 WL 6777384 (D. Minn. Oct. 23, 2015). In *Target*, two forensic investigations were conducted: one for Target's outside and in-house counsel and one for internal purposes, which was shared in part with Target's board of directors. There, the Court held that the report requested by, and issued to, Target's counsel was protected under attorney-client privilege and work-product immunity, but the information related to the report that was shared internally was not protected.

Thus, in the event of a data breach: (1) engage outside counsel immediately; (2) permit outside counsel to hire a forensic firm to conduct an investigation and provide a report related to the data breach for purposes of providing legal counsel;


### Attorneys

Gary Schober


### Practices & Industries

Cybersecurity & Privacy

Intellectual Property & Technology

and (3) do not disseminate the forensic report, or information contained therein, internally (other than in-house counsel, if applicable). This should provide your company with sufficient safe-guards to prevent a data breach forensic report from being discoverable.

If you have any questions about the above cases or information, please contact Jessica L. Copeland or Gary M. Schober.