Privilege Newsletter
Volume 1 | April 18, 2022

Fitting Consultants Within the Attorney-Client Privilege and Work Product Protection – Cyber Breach Consultants

By: David M. Greenwald, Alexander N. Ghantous, Allison M. Tjemsland, Andrew D. Whinery, Effiong K. Dampha, and Sol Gelsomino

Cyber attacks are increasingly frequent and virulent. An intruder may lurk in a company's computer system for years, or an attack may be sudden and catastrophic. Millions of people's personal information and companies' sensitive and proprietary data may be stolen and sold to the highest bidder. And disclosure of a breach ineluctably leads to class action and other civil litigation.

As soon as a breach is detected, companies typically engage outside counsel, who in turn hire third-party forensic computer consultants ("cyber consultants"). When is a cyber consultant's work protected by the attorney-client privilege and the work product doctrine?

Consultants' work may be privileged if the primary purpose of the engagement is to assist counsel with providing legal advice.[1] The *Kovel*[2] doctrine treats consultants as agents of counsel, and within the client's attorney-client privilege, where the consultant is "necessary, or at least highly useful" to counsel's forming legal advice and strategy. The core question is whether the primary purpose of the consultant's work is legal rather than primarily to further business interests. In the wake of a data breach, courts have been reluctant to treat cyber consultants' work as primarily for a legal purpose.

Courts have also been reluctant to apply work product protections. Even where litigation is anticipated or ongoing, work product is protected only if it was prepared "because of" litigation.[3] That is, the consultant's work product would not have been prepared in substantially the same form "but for" the prospect of litigation.[4] The majority of courts have found that cyber consultants' work would have occurred irrespective of the prospect of litigation, and therefore is not protected.

Two early decisions upheld assertions of privilege over computer consultants' work. In *In re Target Corporation Customer Data Security Breach Litigation*,[5] the court found that both the attorney-client privilege and the work product protection were applicable. Target hired two cyber consultants, one to work on an incident response, and one to work directly with counsel. Target asserted privilege only with respect to the second consultant. The second consultant delivered its report directly to counsel and did not share its work with the incident response team. Counsel used the report to form legal strategy, and the company did not distribute the report to non-legal personnel or otherwise use the report for business purposes. Under these circumstances, the court was persuaded the primary purpose of the second consultant's work was legal in nature.

The court in *In re Experian Data Breach Litigation*[6] applied work product protections to a cyber consultant's work. In *Experian*, after learning of a data breach, the company immediately hired outside counsel, who then hired Mandiant to analyze the attack and prepare a report. One day after announcing the data breach, the first complaint was filed against the company. After completing its report, Mandiant delivered the report directly to outside counsel, who then delivered it to in-house counsel. The company demonstrated that counsel actually used the report to develop legal strategy and did not provide the full report to Experian's incident response team or otherwise use the report for business purposes.

In six cases decided since *Experian*, despite counsel engaging the consultants directly, often in the context of litigation, the courts rejected assertions of privilege.[7] Three recent decisions, the most recent in February 2022, reflect factors the courts weigh against finding that the primary purpose of engaging cyber consultants is to assist counsel or prepare for litigation.

In re Capital One Consumer Data Security Breach Litigation[8]: The court rejected application of work product protections and found the following: Capital One entered into a Master Services Agreement ("MSA") with Mandiant in 2015 and thereafter entered into periodic Statements of Work ("SOW") and purchase orders pursuant to the MSA. The SOWs provided for incident response services. A data breach occurred on July 19, 2019. The company engaged outside counsel, who then signed an agreement with Mandiant, which called for computer security incident response and incident remediation services, and incorporated the terms of the 2015 MSA. The court emphasized the fact that, although the agreement provided that the work would be done at the direction of counsel and deliverables would be delivered to counsel, the scope of work was the same as prior SOWs. The court also emphasized that after Mandiant delivered its report to counsel, the report was used for many non-legal purposes. The report was provided to the company's cyber technical, enterprise services, and information security and cyber teams, as well as to the company's regulator (FDIC), the CFPB, the OCC, and the company's independent auditors. Under these circumstances, the court found that the report would have been prepared in substantially the same form in the absence of litigation. Therefore, it could not be said that the report was prepared "because of" litigation.

In re Rutter's Data Security Breach Litigation[9]: Following an alert of a potential data breach, Rutter's engaged outside counsel, who then engaged Kroll "to conduct forensic analyses" and to "determine the character and scope of the incident." In conducting its investigation, Kroll worked alongside Rutter's IT personnel to identify and remediate potential vulnerabilities. Kroll delivered its report directly to Rutter's business personnel and did not first deliver it to counsel. The court found that the report was almost entirely factual in nature, and "where advice and tactics were involved, did not include legal input." In addition to not reflecting a legal purpose, Rutter's corporate representative testified that the company did not anticipate litigation at the time the Kroll report was prepared. Under these circumstances, the court found that Kroll's work was not primarily to prepare for litigation or to enable counsel to provide legal advice.

OTR Transportation, Inc. v. Data Interfuse, LLC[10]: Before addressing waiver, the court found that a forensic computer consultant provided business services, and not services intended primarily to prepare for litigation or to assist counsel in providing legal advice. After discovering a third party had gained unauthorized access to and damaged the company's computer systems, litigation counsel engaged a cyber consultant. The consultant's work was described as "'security consulting solutions.'" The engagement letter provided that work would be performed at the direction of counsel and would be treated as privileged. The court characterized this language as "window dressing," holding that the language of the engagement agreement "does not convert a business services engagement into protected attorney work product." The company's CFO conceded that counsel used only a portion of one status update to draft a complaint. The court found that the consultant's scope of work - to investigate the cause and scope of the intrusion, and to repair the system - was in the ordinary course of business and would have been conducted irrespective of litigation. Even if the consultant assisted counsel with the complaint, that purpose was secondary to the primary business purpose.

In our next newsletter, we address the uphill challenge of protecting communications with third party public relations consultants.

Contact Us

David M. Greenwald
dgreenwald@jenner.com | Download V-Card

Alexander N. Ghantous
aghantous@jenner.com | Download V-Card

Allison M. Tjemsland
atjemsland@jenner.com | Download V-Card

Andrew D. Whinery
awhinery@jenner.com | Download V-Card

Effiong K. Dampha
edampha@jenner.com | Download V-Card

Sol Gelsomino
sgelsomino@jenner.com | Download V-Card

---

[1] *See* David. M. Greenwald & Michele L. Slachetka, *Testimonial Privileges*, §§ 1:29-1:32 (West 2021) for a detailed discussion of third-party agents and representatives (collecting cases).
[2] 296 F.2d 918, 922 (2d Cir. 1961).
[3] *See Testimonial Privileges*, § 2:18 (majority of courts apply the "because of" test).
[4] *Id*.
[5] MDL No. 14-2522 (PAM/JFK), 2015 WL 6777384 (D. Minn. Oct. 23, 2015). You may read the decision here.
[6] SACV 15-01592 AG (DFMx), 2017 WL 4325583 (C.D. Ca. May 18, 2017). You may read the decision here.
[7] *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F.Supp.3d 1230 (D. Or. 2017); *In re Dominion Dental Servs. U.S.A., Inc. Data Breach Litig.*, 429 F.Supp.3d 190 (E.D. Va. 2019); *In re Cap. One Consumer Data Sec. Breach Litig.*, MDL No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238 (E.D. Va. May 26, 2020); *Wengui v. Clark Hill*, PLC, 338 F.R.D. 7 (D.D.C. 2021); *In re Rutter's Data Sec. Breach Litig.*, Civil Action No. 1:20-CV-382, 2021 WL 3733137 (M.D. Pa. July 22, 2021); *OTR Transportation, Inc. v. Data Interfuse, LLC*, Case No. 21 CV 3415, 2022 WL 296056 (N.D. Ill. Feb. 1, 2022).
[8] You may read the decision here.
[9] You may read the decision here.
[10] You may read the decision here.