Privileged Cybersecurity Investigations – A Checklist for Contracting with Consultants

Your company may suffer a cybersecurity incident that warrants bringing in third-party forensics or other consultants to investigate and report on the cause or consequences of the cyber event or compromise. To seek to protect the third parties' reports with the work product privilege (and, thus, to avoid having to disclose the reports in litigation) – and to try to side-step the unexpected failure to establish such protection that Capital One recently experienced (In re: Capital One Consumer Data Security Breach Litigation) – do (and don't do) the following with respect to your contracts with these third parties:

Do have outside counsel be the entity contracting directly with the third party. Have outside counsel pay the third party's fees, directly. Then, have outside counsel bill you for reimbursement of the fees paid.

Do contract under a specific statement of work or services description that is exclusive to the particular cyber incident.

Do state and expressly limit the purpose of the third party's services and reports to anticipating litigation arising from the cyber incident. The purpose should not explicitly or implicitly include, for example, financial controls or reporting.

Do require that the third party's report be in a form and of substance specific to the purpose of anticipating litigation. The report should not mirror what would be provided for

reports for other purposes.

Do require the third party to issue formal and informal reports and updates only to the contracting outside counsel. Outside counsel, then, as necessary or appropriate, can distribute further the reports or updates, for example, to select internal stakeholders.

Don’t allow those who receive reports and updates from outside counsel to further distribute the reports or updates, whether internally or externally. Require recipients to explicitly agree to limited use and handling terms, before receiving reports or updates.

Don’t allocate the costs and fees for the third party’s services to any internal billing or cost center other than Legal’s. The costs and fees should be assigned to Legal’s budget. Categorize the costs and fees as “legal” costs and fees, not, for example, cybersecurity or business costs or fees.

And, in the contract with the third-party forensics firm or consultant, do include requirements that the third party conform to all of the applicable above do’s and don’t’s.

Importantly, these are only a few do’s and don’t’s that may help guide many companies to attempt to structure and implement contracts with third-party consultants so as to establish the work product privilege applicable to the third party’s reports. Each company, each cybersecurity incident, and applicable law can vary and be unique, so it is perhaps even more critical for the company to immediately involve inside (or outside) counsel to navigate these thorny issues.

Background – In re: Capital One Consumer Data Security Breach Litigation

The above do’s and don’t’s follow from the recent decision of the U.S. District Court for the Eastern District of Virginia

in the above-referenced litigation. Capital One sought to avoid having to disclose the report issued by the cybersecurity forensics firm that it retained in wake of the March 2019 data security breach suffered by the financial company.

In affirming a magistrate judge's order to compel Capital One to disclose the forensics report, the Virginia federal district court made several observations. Well before the breach (and not specific to the March breach), Capital One had retained the forensics firm under a general SOW, on a retainer basis, to provide a set number of service hours for any one of a broad range of incident response services that might be needed. After the security breach, although the bank's outside counsel signed a letter agreement with the forensics firm for services with respect to the breach. The terms of the letter agreement provided for the same scope and kind of services, on the same terms and conditions, as the general SOW (except that the forensics firm would work at the direction of the outside counsel and provide the forensics report to the outside counsel).

For performing under the letter agreement, the consultant was first paid from the retainer already provided under the general SOW. Then, Capital One directly paid the balance of the consultant's fees due under the letter agreement – with funds from Capital One's internal general cybersecurity budget. Capital One (at least at first) internally identified the fees paid to the consultant as a "business critical" expense – not as a "legal" expense.

During the forensics firm's investigation, it communicated directly with the bank's external financial auditors, so that the auditor's could assess whether the breach impacted the bank's accounting controls. Many internal and external parties received a copy of the forensics report, but Capital One provided no explanation as to why these recipients received a copy of the report, as to whether the report was provided for

business purposes, regulatory reasons, or specifically in anticipation of litigation, or as to any restrictions placed on the recipients' use, reproduction, or further distribution of the report.

Both the magistrate judge and, on appeal, the district court judge who opined on the matter saw these above facts, among others, as support for finding that the forensic firm's investigation report was not protected from disclosure by the work product privilege.