FOR YOUR EYES ONLY

Preventing the Discoverability of Forensic Reports in Data Breach Litigation

Karen Painter Randall and **Steven Kroll** Connell Foley LLP

Recently, there has been an unprecedented amount of domestic and international activity from government and law enforcement to counter the operations of cyberattacks. Despite these initiatives, threat actors continue to attack enterprises at alarming rates due to the large amount of potential profit. According to statistics released by Coveware in 2021 for Q3, the average cost of a data breach rose to $3.92 million, and the average ransom payment was $139,739. With cybercriminals always seemingly one step ahead, it is not anticipated there will be much of a change in 2022.

A data security breach generally requires the use of outside forensic experts to contain and remediate the incident to ensure an organization's systems are secure. Often the nature and scope of the forensic investigation is memorialized in a formal report. Because one of the potential consequences of suffering a breach is subsequent data breach litigation, an issue that arises is whether these reports, along with the communications surrounding them, are subject to disclosure during discovery. A review of the current trend in federal case law demonstrates that the work product and/or attorney-client privilege may be eroding when it comes to protecting these highly confidential reports. As such, it is important that a great deal of care is used both when communicating with outside experts and in disclosing findings in a report. Moreover, companies must review their protocols for invoking these privileges in light of recent decisions by several district courts.

SUMMARY OF CASE LAW

Until recently, there have been only a few cases dealing with the issue of disclosure of forensic reports prepared after the investigation of a data security incident. In 2015, in In re Target Corp. Customer Data Sec. Breach Litig., a Federal District Court of Minnesota held that a forensic report was protected from disclosure under the attorney-client privilege. In reaching this decision, the court held that the report was prepared for Target's in-house and outside counsel in anticipation of litigation and not for remediation of the breach suffered by Target. Importantly, litigation was already pending and was reasonably expected to continue. Thereafter, in 2017, in In re Experian Data Breach Litig., a Federal Central District of California also denied the disclosure of a forensic report, this time based on the work product doctrine. In particular, the court held that the preparation of the report was intended to assist outside counsel for the affected entity. The court also explained that because the report was not provided to the company's internal incident response team, this was evidence that, but for the anticipated litigation, the report would not have been prepared in substantially the same form or with the same content.

However, the trend has shifted recently. On June 25, 2020, in In re Capital One Consumer Data Sec. Breach Litig., a Federal Court for the Eastern District of Virginia held that a report commissioned by an impacted entity, post-incident, was discoverable because: (1) there was a pre-existing relationship with the forensic vendor and the Scope of Work provision of the contract designated it to be a "business" incident response report; (2) the report was not drafted in anticipation of litigation; (3) dissemination of the report was not limited

to a small number of recipients; and (4) the company paid for the report from a business expense account, not from a legal or litigation budget. Thereafter, on January 12, 2021, in *Wengui v. Clark Hill, PLC*, a Federal Court for the District of Columbia ordered a company to produce its forensic report in discovery, despite the fact its outside counsel ordered the report from the third-party forensic vendor for purposes of investigating the nature, scope and cause of the incident. The court refused to apply either the attorney-client or the work product privilege because the purpose of obtaining the report was investigational, not in anticipation of litigation; nor was the purpose of outside counsel's consultation with the vendor intended to assist in facilitating legal advice.

Most recently, on July 22, 2021, in In re Rutter's Data Security Breach Litig., a Federal Court for the Middle District of Pennsylvania ordered the disclosure of a forensic report where the third-party vendor's Scope of Work was to "conduct forensic analyses on the company's card environment and determine the character and scope of the incident." The court declined to apply the work product privilege because the purpose behind the report was not related to litigation; the attorney-client privilege did not apply because the report was not shown to do more than provide facts regarding exploited vulnerabilities in the system. Put another way, the report did not assist in the provision of legal advice.

STRATEGIES FOR KEEPING FORENSIC REPORTS SECURE

These recent decisions indicate substantial measures are necessary to protect from discovery certain investigative reports or communications with cybersecurity experts. Before engaging an expert, it is imperative to consult with outside counsel to ensure all of the privileges and protections are available by performing the following tasks.

First, an organization should make sure outside counsel is directly involved with the retention of the forensic expert at the outset. Furthermore, outside counsel, not the impacted organization, should retain the expert. This will strengthen the argument that the expert's work, including communications, is for the purpose of assisting counsel.

Second, during the investigation, counsel should be careful to manage verbal and written communications with experts. Several of the court's decisions turned significantly on the recipients with whom the investigative reports were shared. The courts cited the defendants' decision to share the reports with non-lawyers as evidence the reports had essentially non-legal purposes. To that end, companies should disseminate protected reports sparingly and must be able to articulate a legal purpose for sharing the report with each recipient. Accordingly, at the beginning of an investigation, a company should clearly define the incident response team that will assist counsel in providing legal advice. Any communications within this team should be clearly marked as privileged and copied to legal at all times.

Third, the language used in the Statement of Work (SOW) is critical to protecting the work performed by a forensic expert. As noted in one of the recent court decisions, the description of services in the operative letter agreement between the forensic expert and outside counsel should be different than any prior, pre-breach SOW between the security expert and the company. This will demonstrate that the work performed by the expert in response to the data security incident would have been performed regardless of any litigation arising from the specific incident. Where applicable, the SOW should cite specific reasons for the consultant's work related to protecting the company from prospective litigation, since a company's need to analyze its breach reporting obligations, while legal in nature, does not make the investigation report protected work product because such analysis was not in anticipation of litigation. Merely having an SOW between an affected business, a consultant and a lawyer does not automatically create privilege as care must be taken to ensure communications are either in anticipation of litigation or for the purpose of providing legal advice.

Fourth, companies should emphasize the distinction between pre- and post-incident work and enter into entirely new contracts to govern an expert's forensic work following a security incident. Where feasible, companies should consider engaging a separate expert for incident response work to differentiate the scope of work. Accordingly, an organization should consult with outside counsel and prospective cybersecurity consultants prior to an incident occurring as part of formulating an incident response plan to determine the best way to contract for the necessary services in the event of an incident.

Lastly, an organization should anticipate disclosure by a court and prepare to mitigate its impact. A company should limit email and other written communications and determine whether a written report from the cybersecurity expert is necessary before requesting one. Additionally, an organization should not include technical or other remedial recommendations in the investigative report, which could defeat privilege or work product claims on the grounds they are not related to legal advice. Moreover, if the organization cannot follow the recommendations placed in writing, it could potentially be damaging later in discovery. Internal members of the incident response team should be reminded about the importance of maintaining the privilege.

CONCLUSION

The landscape for asserting the attorney-client privilege and/or attorney work product protection to communications and reports prepared by an expert is continuing to evolve. When preparing an incident response plan, a company should consult with outside counsel regarding these recent decisions to ensure their protocols for engaging cybersecurity experts and other vendors are consistent with maintaining privilege should litigation or a regulatory enforcement action follow. These protocols should then be tested through tabletop exercises.

Ultimately, no matter what precautions an organization takes, a court may still determine expert reports and communications during incident response may be discoverable. The steps described above may reduce the risk, as well as mitigate its impact should a court order its disclosure during subsequent data breach litigation.

Karen Painter Randall chairs Connell Foley LLP's Cybersecurity, Data Privacy and Incident Response Group and leads its 24/7 Breach Response Team. Karen has handled hundreds of breach response matters and advises on proactive measures, including security risk assessments, policies/procedures, security awareness training, incident response, tabletop exercises and cyber liability insurance.