SQUIRE PATTON BOGGS

Cyber Breach Forensic Reports: Is Your Report Discoverable?

Although few courts have addressed attorney-client privilege and work product protection in the context of forensic reports, trends have emerged providing insight on how to handle them.

Due to the growing prevalence of data breaches and ransomware attacks, courts have been forced to interpret and nuance privilege in the context of post-breach forensic reports. One major consideration in the context of data breach litigation strategy is how to protect forensic reports prepared by outside forensic firms from discovery in civil litigation. If the forensic report is discoverable, it could be used by the opposing party and ultimately become part of the public record in litigation.

Companies and organizations generally want to maintain privilege over forensic reports because of the likely value to potential plaintiffs. In particular, forensic reports typically identify the likely method by which a threat actor accessed a company's IT environment. In doing so, the report generally highlights critical vulnerabilities in its IT environment. Such information may identify areas in which a company failed to maintain industry standards, thereby potentially breaching its contractual and fiduciary obligations to protect sensitive information.

Courts continue to wrestle with applying conventional legal notions of privilege to novel fact patterns, often resulting in inconsistent or disappointing court decisions. Courts have held that, in certain circumstances, such forensic reports are protected by both attorney-client privilege and work product protection. Although there are few cases discussing these doctrines in the context of forensic reports, the cases provide guidance on what a company or organization can do to bolster claims that its post-breach forensic reports are shielded from discovery in civil litigation.

Attorney-Client Privilege

Only one court has directly addressed whether forensic reports are protected by attorney-client privilege. In *Genesco, Inc. v. Visa U.S.A., Inc.*, a case involving a cyber-attack on a retail store, the defendant's outside counsel engaged a forensic firm to assist with a privileged factual investigation as to how the cyber-attack occurred. The Middle District of Tennessee court found that the attorney-client privilege protects attorneys' factual investigations, and the protection extends to attorneys' communications with agents and experts who are retained for the purpose of providing legal advice. Accordingly, the court held that the report was protected from disclosure by the attorney-client privilege because it was: (1) prepared by the forensic firm at the direction of outside counsel; and (2) prepared to aide counsel in providing legal advice.

Companies should be mindful that attorney-client privilege is easily waived. Subject to a few exceptions, attorney-client privilege is generally waived when the holder voluntarily discloses privileged information to a third party. Thus, to reduce the likelihood that privilege is waived, a company should take care to not disclose the forensic report to any third party, without further guidance from counsel.

Work Product Protection

Multiple federal courts have held that in certain instances, forensic reports are protected by work product protection. Whether a document is work product generally comes down to whether the document was prepared in anticipation of litigation. Although courts use different tests to interpret this phrase, trends have emerged providing guidance on how to obtain work product protection of forensic reports:

- Outside counsel should retain the forensic firm on behalf of the company or organization as opposed to serving as merely a supervisory party after the firm has been engaged by a company; and
- The engagement letter with the forensic firm should include language making sufficiently clear that the purpose of the engagement is to assist outside counsel to prepare for litigation.

Companies should bear in mind that work product protection can be overcome by a finding of substantial need by the adverse party. To strengthen the argument against finding a substantial need, outside counsel should ensure that the forensic firm conducts its investigation based on documentation that can be provided to an adverse party for an independent investigation.

In the wake of a data breach, internal and external parties may seek to obtain a copy of the report. In particular, external parties could include insurance carriers, external auditors, affiliate companies, and regulatory agencies. Internal parties may include a parent company, the incident response team, IT Department, and vendors or consultants retained by outside counsel.

In contrast to attorney-client privilege, work product protection is not automatically waived by disclosure to a third party. To determine whether work product protection is waived, most courts distinguish between disclosures to an adversary versus a non-adversary. This approach has been used in the context of forensic reports as the court in *In re Experian Data Breach Litig.* held that forensic reports may be disclosed to third parties so long as the disclosure is "consistent with maintaining the secrecy against opponents."

Recognizing that disclosure to selective third parties may be an appropriate business decision, companies can take precautionary measures to reduce the risk that work product protection will be waived, including:

- Redacting the report as much as possible;
- Requiring the receiving party to sign a confidentiality agreement; and
- If applicable, entering into a common interest agreement with the receiving party.

Even so, providing a forensic report to a third party increases the risk of wavier. Therefore, companies should maintaining tight control over to whom disclosure of a forensic report is made and consult with counsel before doing so.

Companies should also consider whether waiving protection vis-à-vis one potential adversary waives work product protection in litigation with future adversaries. Although this issue has not been addressed by the courts in the context of forensic reports, under the traditional analysis, federal courts use different tests to determine whether a party may selectively waive privilege.

Although few courts have addressed attorney-client privilege and work product protection in the context of forensic reports, trends have emerged providing insight on how to handle forensic reports. Due to the growing prevalence of data breach litigation and the importance of shielding forensic reports from potential plaintiffs, this is an area of law likely to be addressed by courts in the near future.

Leah K. Parsons is an associate at Squire Patton Boggs, focusing primarily on corporate matters, including mergers and acquisitions, venture capital transactions and corporate governance.

Ericka A. Johnson is an associate at Squire Patton Boggs, where she represents companies and executives in, among other things, Foreign Corrupt Practices Act (FCPA) internal investigations, enforcement actions, defense matters and compliance before the US Department of Justice and similar authorities. As part of her compliance practice, Ericka advises companies on cybersecurity risks, internal compliance measures and incident response protocols.

Colin R. Jennings is a partner at Squire Patton Boggs, where his practice focuses on global compliance work for public and privately held companies. In addition to his operations compliance work, Colin offers investigation and defense of compliance-related concerns. As a natural extension of his practice, Colin has an active data privacy and breach response practice, and he regularly interacts with federal, state and international authorities concerning data breaches, as well as coordinates the forensic analysis and resulting claims or litigation that inevitably follow a breach.

Contacts

Colin Jennings
Partner, Cleveland
T +1 216 479 8420
E colin.jennings@squirepb.com

Ericka Johnson
Associate, Washington DC
T +1 202 457 6110
E ericka.johnson@squirepb.com

Leah Parsons
Associate, Denver
T +1 303 894 6107
E leah.parsons@squirepb.com