SIDLEY

JANUARY 26, 2018

SIDLEY UPDATE

Protecting Privilege in the Aftermath of a Data Breach

On Jan. 3, the United States Court of Appeals for the Sixth Circuit issued a decision that effectively required a company to turn over materials relating to a privileged forensic data breach investigation because, the court concluded, the company had implicitly waived privilege when it disclosed certain of the forensic firm's conclusions in response to a discovery request. The Sixth Circuit's decision emphasizes the need for caution by litigants wishing to raise a defense that relies on privileged investigations and reports, including third-party forensic reports, or otherwise disclosing the conclusions of such investigations and reports.

In the aftermath of a significant data security incident, a best practice is to hire a third-party forensic firm, working at the direction of counsel, to review how the breach occurred, what data may have been accessed, whether the incident has ceased and other important issues directly relevant to legal counsel's review. When privilege protocols are followed, attorney-client and, if applicable, work-product protections will generally cover the investigation as well as reports, communications and other materials relating to the investigation. The Sixth Circuit's decision has important implications for how forensic investigation findings and conclusions should be handled.

In *Leibovic v. United Shore Financial Services, LLC,* the plaintiff filed a putative class action against United Shore Financial Services (United Shore) and Xerox Mortgage Services, Inc. (XMS) over alleged intrusions into XMS's systems on which United Shore had stored potential borrowers' personal information. In response, United Shore raised several affirmative defenses, including that the plaintiff's claims against United Shore were barred based on co-defendant XMS's alleged acts or failures to act.

As part of its response to a suspected cybersecurity incident, counsel for United Shore hired a forensic firm to investigate and analyze the suspected incident. Subsequently, during discovery in the civil suit, United Shore was asked to state with particularity all investigations and remedial efforts taken in relation to the alleged intrusions. In response, the company disclosed its engagement of the forensic firm and further disclosed certain of the firm's conclusions, which, the district court later observed, United Shore intended to use to support its affirmative defense concerning XMS's alleged acts or failures to act. See Order, *Leibovic v. United Shore Fin. Servs., LLC,* No. 15-12639, 2017 BL 301590, at *4 (E.D. Mich. Aug. 28, 2017). But, citing attorney-client privilege, United Shore withheld hundreds of documents relevant to the forensic firm's investigation. XMS moved to compel United Shore to produce the withheld documents, arguing that United Shore had implicitly waived the attorney-client privilege by disclosing the investigation's conclusions.

The district court granted XMS's motion and denied United Shore's subsequent motion to clarify its order. See, e.g., *id.* at *1. Specifically, the district court reasoned that United Shore's responses to discovery requests

"went beyond providing factual information regarding the existence of the investigation and retention of [the firm]" and "also included details regarding [the firm's] conclusions," which exceeded the scope of the discovery request. See *id.* at *3. According to the district court, "United Shore fail[ed] to explain 'why the conclusions of a supposedly privileged investigation commissioned by counsel would not themselves be privileged.' " Thus, because United Shore disclosed privileged conclusions and it appeared that the company intended to use the investigation findings to prove the ultimate cause of the alleged intrusion, XMS was entitled to "documents related to how the investigation was conducted and what was considered during the investigation," including communications between the company and/or its counsel and the forensic firm (to the extent responsive to the interrogatory at issue). See *id.* at *3–4.

On appeal, the Sixth Circuit denied United Shore's petition for a writ of mandamus and found that the district court had correctly concluded that the attorney-client privilege had been implicitly waived. The Sixth Circuit opinion explained, " 'Litigants cannot hide behind the privilege if they are relying on privileged communications to make their case' or, more simply, cannot use the privilege as 'a shield and a sword.' " *In re United Shore Fin. Servs., LLC*, 2018 BL 1881 (6th Cir. 2018) (citing *In re Lott*, 424 F.3d 446, 454 (6th Cir. 2005); *United States v. Bilzerian*, 926 F.2d 1285, 1292 (2d Cir. 1991)). " 'Thus, the privilege may be implicitly waived when a defendant asserts a claim that in fairness requires examination of the protected communications.' " *Id.* (quoting *Bilzerian*, 926 F.2d at 1292).

This case underscores the importance of remaining sensitive to the privileged nature of forensic investigations in the aftermath of a breach, particularly in the context of litigation and regulator inquiries that often follow. The likelihood of maintaining privilege and work product protections increases if companies take certain precautions. Accordingly, clients should consider the following steps to prevent inadvertent waiver of privilege or to at least help limit the scope of disclosure when it cannot be avoided:

- Work with legal counsel in investigating the facts and circumstances of a breach, and make clear that the investigation — including the use of third-party forensic firms — is being conducted at the direction of legal counsel, to provide legal advice and/or in anticipation of litigation.
- Have counsel engage the forensic firm directly, on behalf of and as counsel for the company, and explicitly note in the engagement letter that the forensic firm is working at the direction of counsel.
- Clearly define the goals and the scope of the investigation at the outset, including in applicable engagement letters, and ensure that those involved with the investigation have a clear understanding of the scope.
- When disclosing matters relating to the investigation, limit such disclosures to facts alone, not findings, conclusions, protected communications or other matters of judgment, unless the company has carefully weighed and considered the benefits and risks of making such disclosures and potentially waiving the privilege.
- To the extent disclosure is necessary, take care to avoid overbroad disclosures.
- Remember that there is no guarantee that an investigation will remain confidential — for instance, information may be leaked or inadvertently disclosed, or a company may choose to waive privilege in favor of disclosure down the road — so be mindful of this possibility when creating or handling communications and other materials during the course of the investigation.

If you have any questions regarding this Sidley Update, please contact the Sidley lawyer with whom you usually work or

Geeta Malhotra
Partner
gmalhotra@sidley.com
+1 312 853 7683

Edward R. McNicholas
Partner
emcnicholas@sidley.com
+1 202 736 8010

Alan Charles Raul
Partner
araul@sidley.com
+1 202 736 8477

Elizabeth MacGill
Associate
emacgill@sidley.com
+1 202 736 8546

Clayton G. Northouse
Associate
cnorthouse@sidley.com
+1 202 736 8131

Sidley Privacy and Cybersecurity Practice

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes lawyers experienced in regulatory compliance, litigation, financial institutions, healthcare, EU regulation, IT licensing, marketing counsel, intellectual property and criminal issues. Sidley provides services in the following areas:

- Privacy and Consumer Protection Litigation, Enforcement and Regulatory Compliance
- Data Breach, Incident Response and Cybersecurity Advice, Response and Litigation
- Global Data Protection, International Data Transfer Solutions and Cross-Border Issues
- Corporate Data Protection, Compliance Programs and Information Governance Assessments
- FTC and State Attorney General Investigations of Unfair or Deceptive Acts and Practices
- Cloud Computing, Social Media, Online Advertising, Internet of Things, E-Commerce and Internet Issues
- EU, China, Japan, Singapore, Hong Kong and other International Data Protection and Compliance Counseling
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy
- Communications Law and Data Protection
- Workplace Privacy and Employee Monitoring
- Website Policies, Online Trademarks and Domain Name Protection
- Records Retention, Electronic Discovery and Defensible Deletion
- Governmental Access and National Security

To receive Sidley Updates, please subscribe at www.sidley.com/subscribe.