Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Why Counsel Should Direct Your Data Security Investigations

Law360, New York (April 09, 2015, 5:10 PM ET) --

Alfred Saikali

Reports generated from privacy and security audits and data breach investigations often contain unintentionally harmful statements about a company's security safeguards or privacy practices. Frequently these documents contain opinions on issues such as when a breach began or ended, when it should have been discovered, whether regulated data was accessed or acquired, and whether the company was engaging in reasonable security practices — critical topics for regulators and plaintiffs attorneys. Courts are recognizing, however, that when those audits and investigations are directed by counsel to evaluate a company's legal rights and obligations they are subject to the same protections from disclosure as any other attorney-client communication.

The Middle District of Tennessee recently held that documents related to a compliance-related network security audit performed by a third party — and managed by counsel — were protected from disclosure by the attorney-client privilege. The district court's March 25 order is the latest in a dispute between Genesco Inc. — parent company to retail brands Journeys and Lids — and payment-card network provider Visa.

In 2010, hackers targeted Genesco's payment card system, focusing on card data as it was transmitted to two of the retailer's payment card issuing banks. Visa levied nearly $13.3 million in fines against the banks for Genesco's alleged violations of the Payment Card Industry Data Security Standards, including an alleged failure to ensure that Genesco was compliant with PCI standards at the time of the breach. In standard industry practice, the banks then collected the assessed amounts from Genesco directly. In an industry first, however, Genesco challenged Visa's legal authority to impose such fines.

During discovery, Visa sought to compel production of documents related to security assessment and remediation work performed by third-party vendors, including IBM, on Genesco's behalf. Genesco retained these third parties through in-house and outside counsel to provide consulting and technical services that would help Genesco remediate issues uncovered by a third-party audit as well as understand and meet its PCI DSS compliance obligations. Visa argued that the work performed by these vendors constituted factual material not protected by the attorney-client privilege.

Denying Visa's motion to compel, the court found that, while relevant to the litigation at hand, the materials sought were protected by the attorney-client privilege because counsel retained IBM to provide consulting services in assistance with rendering legal advice to the client. Nor were the prepared reports subject to the waiver provision of Federal Rule of Civil Procedure 26(b)(4)(D), which provides for the disclosure of expert reports where it is "impracticable" for the opposing party to obtain the information by other means.

Numerous courts outside the data security context have held that the attorney-client privilege and work-product doctrine protect documents created in similar arrangements, i.e., where counsel serves as a legal filter for communications between the client and third parties that provide technical expertise necessary to answer a legal question.[1] As shown in cases such as Kovel, this extension of the attorney-client privilege has been an established legal doctrine since at least the 1950s. Factual investigations have repeatedly been protected from discovery pursuant to the attorney-client privilege and work-product doctrine. Courts will deny application of the privilege, however, when the attorney merely acts as a conduit for analysis performed by the third-party investigator.[2] Accordingly, the attorney must be mindful that information obtained through the third party is filtered through her own legal analysis.

Furthermore, the presumption of privilege is strengthened when outside counsel, rather than in-house counsel, directs and manages the third-party relationship. and information flow between experts and client.[3] The distinguishing feature between outside counsel and in-house counsel retaining the expert is that communications between a client and its outside counsel are made for the purposes of obtaining legal advice. This stands in contrast to corporate communications involving in-house counsel, as such individuals are frequently involved in the day-to-day business activities of the company and often are key decision-makers in operational or strategic matters. Because the attorney-client privilege does not extend to an attorney's business advice, courts often require a stronger showing — and consequently a deeper court inquiry into supporting documents — that communications between an in-house attorney and other corporate decision makers involved the attorney's functions.[4]

Plaintiffs lawyers are increasingly filing class actions against companies that have suffered a data breach. Inevitably, these lawsuits are accompanied by discovery requests seeking forensic reports, security audits and internal privacy policies. And litigation is not the only front where these documents are sought, as post-incident regulatory investigations often include a demand for materials generated during any post-breach forensic audits. Indeed, several state breach notification laws explicitly give those state attorneys general the authority to request any post-breach forensic audits conducted by the breached entity.

In the face of this increased pressure to disclose the results of internal investigations, the attorney-client privilege and work-product doctrine remain important tools to challenge such discovery. Companies should carefully consider the engagement of external counsel to direct information security assessments, regulatory compliance audits, and breach response investigations to preserve privilege and work-product protection over potentially damaging documents. External counsel's management of these investigations carries with it the presumption of privilege, which both mitigates the risk of future disclosure and permits the breached entity to receive and interpret the information provided in the most efficient manner possible to manage a security incident and its aftermath.

—By Alfred Saikali and Eric S. Boos, Shook Hardy & Bacon LLP

Al Saikali is a partner in Shook Hardy & Bacon's Miami office and chairs the firm's data security and privacy practice group. Eric Boos is an associate in the firm's Miami office.

[1] See Gucci America, Inc. v. Guess? Inc., 271 F.R.D. 58, 70 (S.D.N.Y. 2010) (citing the foundational United States v. Kovel, 296 F.2d 918 (2d Cir. 1961) for its extension of the attorney-client privilege to an accounting hired by outside counsel to assist in representation of client).

[2] See, e.g. United States v. Ackert, 169 F.3d 136, 139-40 (2d Cir. 1999) (no privilege when advice provided to client was that of an investment banker and not that of the attorney).

[3] See, e.g. United States v. ChevronTexaco Corp., 241 F. Supp. 2d 1065, 1076 (N.D. Cal. 2002)(“communications involving in-house counsel might well pertain to business rather than legal matters” and accordingly “the presumption that attaches to communications with outside counsel does not extend to communications with in-house counsel”).

[4] Id. (“In-house counsel may be involved intimately in the corporation's day to day business activities and frequently serve as integral players in business decisions or activities ... The privilege does not protect an attorney's business advice.”).
