PRIVACY AND DATA SECURITY ALERT

APRIL 8, 2015

SHOOK
HARDY & BACON

WHY YOUR DATA FORENSIC INVESTIGATIONS SHOULD BE DIRECTED BY COUNSEL

Reports generated from privacy and security audits and data breach investigations often contain statements about a company's security safeguards that can be unintentionally harmful to a company on issues like when a breach should have been discovered and whether the company was engaging in reasonable security practices. 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 protected from disclosure. A recent federal court decision underlined the importance of conducting these investigations through counsel.

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 order** is the latest in a hotly contested dispute between Genesco, Inc.—parent company to retail brands Journeys and Lids—and payment-card network provider VISA. After a 2010 data breach, VISA levied nearly $13.3 million in fines against Fifth Third Bank and Wells Fargo Bank, issuing banks for the payment cards involved in the breach, for violations of the Payment Card Industry Data Security Standards (PCI DSS). In standard industry practice, the banks then collected the assessed amounts from Genesco directly. In an industry first, however, Genesco challenged VISA's authority to impose such fines.

During discovery, VISA sought to compel production of documents related to security assessment work performed by IBM on Genesco's behalf. Genesco had retained IBM to provide consulting and technical services to assist with understanding and meeting the company's PCI DSS compliance obligations at the direction of Genesco's in-house and outside counsel.

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.

Shook, Hardy & Bacon understands companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

For more information about Shook's data security and data privacy services, please contact:

Al Saikali
305.960.6923
asaikali@shb.com

Eric Boos
305.358.5171
eboos@shb.com

Numerous courts outside the data security context have applied attorney-client privilege and work product protection to the work product of similar arrangements, i.e. where counsel serves as a legal filter for communications between individuals providing technical expertise necessary to answer a legal question and the client. *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 representing client). Of course, the presumption of privilege is strengthened when outside counsel, rather than in-house counsel, manages the third-party relationship and information flow between experts and client. *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").

Plaintiffs' lawyers are increasingly filing class action lawsuits 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. Nevertheless, the attorney-client and work-product privileges remain an important tool to challenge such discovery. In this climate, companies should carefully consider the engagement of external counsel to direct information security assessments, regulatory compliance audits, and breach response investigations to preserve privilege over potentially damaging documents and allow the engaged consultants to provide the open and honest feedback required to efficiently manage a security incident and its aftermath.