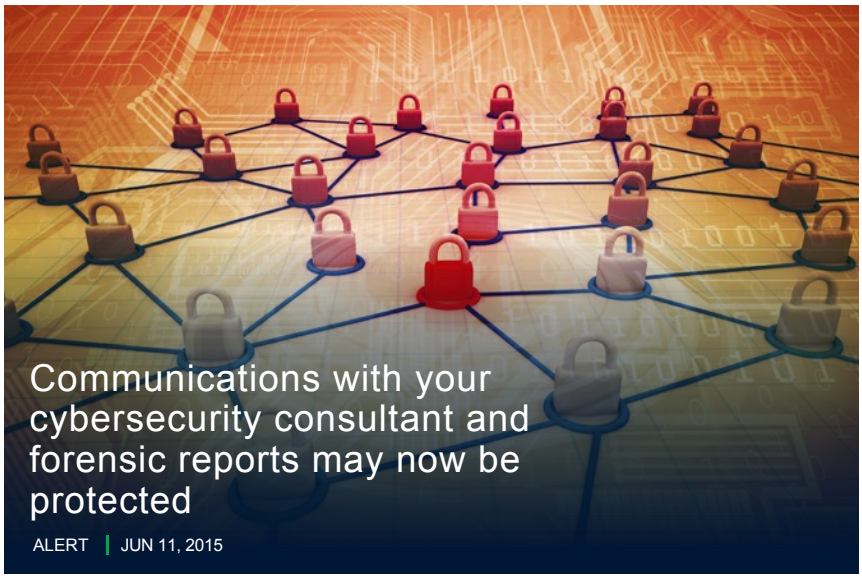


# Communications with your cybersecurity consultant and forensic reports may now be protected

ALERT | JUN 11, 2015

A recent ruling in Tennessee will prove key for cybersecurity litigation everywhere. In *Genesco, Inc. v. Visa U.S.A.*, the court ruled that when cybersecurity consultants and forensic experts are engaged through counsel, the advice and forensic reports they give to a client are subject to attorney-client and work product privilege.

Specifically, in this one-to-watch case, the court denied Visa's requests for analyses, reports, and communications made by two cybersecurity firms Genesco retained after it suffered a data breach, finding that those materials were protected by the attorney-client privilege and work product doctrine.

## WHAT THIS DECISION MEANS TO YOU

Cybersecurity assessments and incident response efforts require careful consideration. These measures bring potential brand and reputation issues, regulatory enforcement and compliance risks, possible litigation, and other challenges that may drive and impact preparedness and response efforts.

The court's decision demonstrates how important it is for you to designate experienced privacy counsel to lead cybersecurity initiatives, including determining proactive privacy and security measures, directing forensic investigations, and spearheading data breach response efforts. Experienced privacy counsel understands the legal significance of the decisions being made. And, more importantly, when your counsel brings in cybersecurity consultants to deal with forensics or other matters, those communications are arguably privileged and protected from disclosure.

You should embrace the significant impact counsel can have on your efforts in cybersecurity risk assessment, mitigation, and incident response strategies. Take advantage of attorney-client privilege and work product protections that attach to their work. By utilizing privacy counsel, you have a safe space to discuss significant – and in some cases bet-the-farm – data privacy and cybersecurity protections, remediation, and vulnerabilities. This safe space allows you to obtain the most accurate information about your cybersecurity posture. It also allows for an open and honest discussion about where you stand so you can ensure you take all appropriate efforts to prepare for a breach, respond to an incident, or prepare for litigation and regulatory enforcement actions.

## A QUICK REVIEW OF THE CASE

Genesco is a retailer with over 2,400 stores throughout the U.S. and internationally. Visa agreed to operate Genesco's retail electronic payments and facilitate payment to financial institutions and businesses for consumer credit and debit card purchases. In their agreement, Genesco agreed to comply with Visa's International Operating Regulations (VIOR) and the Payment Card Industry Data Security Standards (PCI DSS), which establish data security standards for companies that process, store, or handle card data. In contracts with its acquiring banks, Genesco agreed to indemnify them for all fees, assessments, and penalties imposed on them by Visa.

From December 2009 to December 2010, hackers accessed Genesco's computer network, utilizing malware that captured unencrypted credit card data at the point of sale as the data was being transmitted to banks for authorization. After the breach was discovered, Visa claimed every card Genesco processed over a one-year period was compromised. Visa levied fines against the banks to the tune of $13.3 million, which Genesco had to pay. Genesco sued Visa to recoup the amounts under various theories.

During its breach remediation efforts, Genesco hired two cybersecurity firms to provide technical and consulting services to its outside privacy counsel. One worked on alleged past violations of PCI DSS. The second worked on Genesco's ongoing efforts to comply with PCI DSS.

In discovery, Visa moved to compel information regarding the forensic/cyber consulting services, claiming it was entitled to information concerning "Genesco's investigation, analysis, and reviews...in relation to the [cyberattack], including but not limited to those performed internally or through vendors or service providers; communications and reports relating to the first cybersecurity firm's analysis of the purported PCI DSS violations; and the second firm's post-cyberattack PCI DSS compliance analysis."

## THE DECISION

The reasoning behind the court's decision to deny the information request is significant. First, the court ruled that the requested materials were protected under the attorney-client privilege because "attorneys' factual investigations fall comfortably within the protection of the attorney-client privilege," and "[t]his privilege extends to the [cybersecurity] firm that assisted counsel in its investigation." The court reasoned that essentially, cybersecurity and forensic consultants are no different than accounting consultants, whose work product and communications have traditionally been held to be subject to the attorney-client privilege because the "concepts are a foreign language to some lawyers in almost all cases... [h]ence...the presence of the [consultant] is necessary, or at least highly useful, for the effective consultation between the client and the lawyer which the privilege is designed to permit."

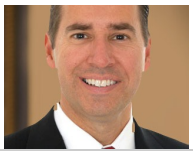
The court went further and also held that the forensic reports were protected under the work product privilege which "attaches to an agent's work under counsel's direction," since "attorneys must often rely on the assistance of investigators and other agents in the compilation of materials in preparation for trial."

For more information, please contact one of the attorneys listed below.

---

JAMES GISZCZAK

## Data Privacy and Cybersecurity Communications with your cybersecurity consultant and forensic reports may now be protected



**Read More**

DOMINIC PALUZZI

**Read More**