LITIGATION NEWS
NEWS, ANALYSIS, AND PUBLICATIONS FROM THE ABA SECTION OF LITIGATION

Home › Litigation News › Top Stories

Merchants May Have Recourse on Data Breach Liability Assessments
By Henry R. Chalmers, Litigation News Associate Editor - October 10, 2013

In a decision likely to have ripple effects throughout the nation’s retail industry, a federal court in Tennessee allowed a merchant to maintain claims against Visa to recoup liability assessments imposed due to a data breach of the merchant’s point-of-sale payment processing system. Genesco, Inc. v. Visa, U.S.A., Inc. [PDF]. This may become the first successful claim by a merchant directly against a payment network to reverse such assessments.

Underlying Business and Contractual Relationships
Like other payment networks, Visa operates an international payment system for its credit and debit cards (payment cards). Visa enters into licensing arrangements with various financial institutions (issuing banks, or issuers) that issue the payment cards to cardholders. Cardholders then use the cards to make purchases.

Merchants that accept payment cards, like plaintiff Genesco, Inc., contract with other financial institutions (acquiring banks, or acquirers) and payment card processors to process and collect the payments from the cards’ issuing banks. The issuing banks send the cardholders monthly credit card statements.

Hanging over these series of relationships is the ever-present specter of a data breach to a merchant’s payment system. If hackers penetrate a merchant’s payment system and extract payment card information, they can use the information to manufacture counterfeit cards and make fraudulent charges to the cardholders’ accounts. Leading studies conclude that more than 170 million records [PDF] were compromised worldwide in 2012, many of them payment card accounts, costing the breached companies approximately $136 per record ($188 each in the United States) [PDF].

Visa and other payment networks attempt to combat breaches by requiring the acquiring banks to ensure participating merchants implement and follow the Payment Card Industry’s Data Security Standards (PCI DSS) [PDF]. The acquiring banks must also agree that, in the event of a data breach, Visa may impose liability assessments on the acquiring bank for its failure to adequately ensure the merchant’s PCI DSS compliance. The acquiring banks, in turn, require their participating merchants to indemnify them for all such assessments.

Data Breach Between Merchant and Acquiring Bank
The merchant, Genesco, Inc., experienced a year-long data breach in which hackers stole customers’ payment card account data as Genesco transmitted it, unencrypted, to the acquiring banks, Wells Fargo Bank and Fifth Third Financial Corporation, for payment authorization. Upon identifying the breach and a corresponding increase in payment card fraud, Visa imposed more than $1.3 million in contract-based liability assessments on Wells Fargo and Fifth Third. The banks then recouped the money from Genesco.

"Payment card processors and, by extension, the merchants for which they provide services stand exposed to such liability assessments whenever a merchant, by failing to comply with applicable data security standards, is subject to a data breach,” says Edward A. Marshall, Atlanta, cochair of the Payment Systems Subcommittee of the ABA Section of Litigation’s Commercial and Business Litigation Committee. "Many merchants and their counsel are not even aware of such exposure until they learn of a data breach," Marshall adds.

Merchants who contend their payments should not have been withheld are usually limited to challenging the assessments with their acquiring banks and processors. This is largely because merchants have no contractual relationships or direct lines of communication with the payment networks. Merchant lawsuits against payment networks are rarely successful due to the strength of the underlying indemnification agreements between the merchants and the banks. In a novel approach for the industry, however, Genesco purchased from
Wells Fargo and Fifth Third assignments of any claims for reimbursement the banks might have against Visa.

**Genesco’s Claims Survive Motion to Dismiss**

Genesco sued Visa in the U.S. District Court for the Middle District of Tennessee to recoup the liability assessments. Visa moved to dismiss on the ground that the provisions of Visa’s contracts with Wells Fargo and Fifth Third preclude Genesco’s claims for restitution.

The district court denied Visa’s motion to dismiss Genesco’s claims under California’s Unfair Competition Laws and for restitution. Genesco contends that Visa had no basis to impose liability assessments based on alleged violations of the PCI DSS, as the Standards—according to Genesco—do not require encryption of data being transmitted to acquiring banks. Genesco also asserts there is no forensic evidence that hackers were able to steal payment card information stored within Genesco’s computer system, where encryption is required. Genesco further contends that Visa calculated the assessments based on each cardholder account that Genesco processed during the year-long data breach. Genesco asserts, however, that forensic evidence shows that at least some of those accounts were never compromised.

“To the extent Visa’s contracts effectively permit fines and assessments upon banks and merchants without factual predicates,” the district court ruled, “the imposition of those fines and assessments could be found to be an unfair and unlawful business practice.”

Focusing its sights more broadly, the court also concluded that Genesco’s allegations “create a controversy that allegedly impacts the operation of the Visa card payment system and implicates consumers, merchants and other banks impacted by the cyber attack on Genesco’s computer network.” Visa’s contracts with acquiring banks, the court opined, “create a structure or ‘environment’ that could be found to be harmful to competition at the merchant level and establish unfairness in the market for credit and debit card transactions of which merchants and consumers are key players.”

“This decision could have wide-ranging implications for future litigation against payment networks,” says Stephen J. Siegel, Chicago, cochair of the Section of Litigation’s Commercial and Business Litigation Committee. “Once the policies behind unfair competition laws are implicated, the lack of a direct contractual relationship may be less of an impediment to merchant lawsuits.”

The decision “has the potential to upset a carefully crafted paradigm for addressing merchant data breaches,” Marshall observes. “The covert nature of hackers’ activities, and the number of cardholders impacted by a data breach, have always made traditional litigation between affected parties highly inefficient, if not outright impossible.”

**Keywords**: data breach, payment cards, credit cards, PCI DSS

---

**Related Resources**

* [Verizon Data Breach Investigations Report] [PDF],
* [Ponemon Institute, 2013 Cost of Data Breach Study: Global Analysis] [PDF],
* [Payment Card Industry Data Security Standards] [PDF].

---

**Comments**

Be the first to comment.

---

**Add Comment**

We welcome your comments. Please use the form below to post.

Name

Email

Comment

Submit