Payment Processor's "In-House" PCI Compliance Program Under Attack

Edward A. Marshall

In the wake of recent and highly publicized data breaches involving payment card information, businesses accepting payment cards (or "merchants") are becoming increasingly sensitive to ensuring compliance with applicable data security guidelines, known as the Payment Card Industry Data Security Standard or PCI DSS. After all, if a merchant suffers a data breach due to its failure to adhere to PCI standards, it can face staggeringly large liability assessments from card brands, such as Visa and MasterCard, associated with resultant payment card fraud.

For years, PCI compliance service vendors, which receive certification by the PCI Council—a body originally formed by American Express, Discover, JCB, MasterCard, and Visa—have assisted merchants with ensuring their fidelity to PCI DSS. To gain access to these merchants, such service vendors frequently collaborate with payment card processors and acquirers, *i.e.*, the entities that contract with individual merchants and/or independent sales organizations ("ISOs") and facilitate the authorization and payment of card transactions.

More recently, however, certain processors have developed their own "in-house" PCI compliance programs, which they provide to certain merchants for a fee. One such program offered by First Data recently came under attack in litigation involving a service vendor with which First Data had historically contracted to provide PCI compliance services.

Specifically, in *First Data Merchant Services Corp. v. SecurityMetrics, Inc.*, Civil Action No. RDB-12-2568 (D. Md. 2012), First Data brought suit against its former service vendor, SecurityMetrics, claiming that SecurityMetrics had engaged in a campaign of false advertising and unfair business practices against First Data following the termination of the parties' contractual relationship. SecurityMetrics counterclaimed, contending that First Data's recently introduced and competitive PCI compliance service solution, "PCI Rapid Comply," was unlawful for a host of reasons. In a recent ruling, the District Court rejected First Data's arguments that several of these counterclaims should be dismissed for failure to state a claim—a decision that may give other processors pause as they seek to implement similar in-house PCI compliance solutions.

Among other things, SecurityMetrics alleged that First Data's use of the phrase "PCI" in the title of its program was likely to cause merchants to incorrectly perceive First Data's program as one explicitly endorsed by the PCI Council, when that was not the case. According to SecurityMetrics, this "false endorsement" violated Section 43 of the Lanham Act.

First Data argued that the claim should be dismissed because SecurityMetrics owned no mark confusingly similar to First Data's "PCI Rapid Comply" mark, and thus, from First Data's perspective, SecurityMetrics lacked standing to pursue a Lanham Act claim. The court disagreed. Rather, it held that persons with standing under Section 43 of the Lanham Act extended beyond holders of similar marks. According to the court, because Section 43(a)(1) of the Lanham Act defines a potential plaintiff as "any person who believes that he or she is or is likely to be damaged by [the defendant's] act[,]" SecurityMetrics—which had alleged "damage[ ] to its commercial interests and its ability to stay competitive in the marketplace"—pled facts sufficient to support its standing.

What is more, the court declined to dismiss counterclaims brought by SecurityMetrics alleging an unlawful restraint on trade in violation of Section 1 of the Sherman Act and attempted monopolization in violation of Section 2 of the Sherman Act.

According to SecurityMetrics, First Data had contracts with ISOs, *i.e.*, third-party sales organizations that market, open, and manage merchant processing accounts for acquirers and payment processors, that imposed billing minimums on the ISOs. Fees paid to First Data for use of its PCI Rapid Comply program would count towards those billing minimums, while fees paid to other service vendors would not. From SecurityMetrics' perspective, this constituted an unlawful "tying" arrangement in violation of Section 1 of the Sherman Act, which proscribes certain anticompetitive restraints on trade. Holding that SecurityMetrics had adequately stated such a claim, the court rejected First Data's argument that SecurityMetrics had failed to allege a necessary element of the tying claim, *i.e.*, "an agreement conditioning purchase of the tying product upon purchase of the tied product (or at least upon an agreement not to purchase the tied product from another party)." According to the court, the allegations describing the aforementioned billing structure—under which fees paid for the PCI Rapid Comply would count towards billing minimums, but fees paid to other service vendors would not—sufficed to describe an unlawful "tying arrangement," at least at the pleadings stage. The court also declined to dismiss the Section 1 Sherman Act claim on grounds that SecurityMetrics had purportedly failed to allege an actionable agreement to restrain trade or market-wide anticompetitive effect.

Likewise, the court permitted the Section 2 Sherman Act claim to survive a pleadings-stage attack. Although finding SecurityMetrics' allegations insufficient to show the monopoly power needed to sustain an outright monopolization claim, the court held that SecurityMetrics had alleged enough to state an *attempted* monopolization claim, which requires only a showing that the defendant used anticompetitive conduct with the specific intent to monopolize and a dangerous probability of success. In reaching this conclusion, the court focused on SecurityMetrics' allegations of "exclusionary conduct" by First Data, including allegations of tying, predatory pricing, and false statements purportedly designed to mislead SecurityMetrics' customers.

At this stage of the case, the ultimate success or failure of SecurityMetrics' counterclaims is impossible to predict. Nevertheless, the Maryland court's decision will likely give processors and acquirers understandable unease as they attempt to implement their own PCI compliance solutions. At a minimum, the outcome of the case could have significant impacts on the marketing and fee structures associated with such "in-house" PCI compliance services.

Authors and Contributors

Edward A. Marshall
Partner, Atlanta Office
404.873.8536
edward.marshall@agg.com

not *if*, but *how*.®

About Arnall Golden Gregory LLP

Arnall Golden Gregory, a law firm with more than 150 attorneys in Atlanta and Washington, DC, employs a "business sensibility" approach, developing a deep understanding of each client's industry and situation in order to find a customized, cost-sensitive solution, and then continuing to help them stay one step ahead. Selected for The National Law Journal's prestigious 2013 Midsize Hot List, the firm offers corporate, litigation and regulatory services for numerous industries, including healthcare, life sciences, global logistics and transportation, real estate, food distribution, financial services, franchising, consumer products and services, information services, energy and manufacturing. AGG subscribes to the belief "not if, but how.®" Visit www.agg.com.

Atlanta Office
171 17th Street NW
Suite 2100
Atlanta, GA 30363

Washington, DC Office
1775 Pennsylvania Ave., NW,
Suite 1000
Washington, DC 20006

To subscribe to future alerts, insights and newsletters: **http://www.agg.com/subscribe/**