

Visa struck back at Heartland on Thursday (March 12), suspending [the data breach victim](#) and removing it from Visa's online list of PCI DSS compliant providers. Visa's chief enterprise risk officer, Ellen Richey, told banks the news in an E-mail Thursday.

Richey described Heartland's status as being "in a probationary period," during which it can still accept payments, assuming it meets various new requirements. Heartland "is now in a probationary period, during which it is subject to a number of risk conditions including more stringent security assessments, monitoring and reporting. Subject to these conditions, Heartland will continue to serve as a processor in the Visa system."

Heartland issued a statement Friday (March 13) that didn't address Visa's suspension, but was clearly prompted by it. "Heartland Payment Systems is pleased to continue our long relationship with Visa. Heartland is cooperating fully with Visa and other card brands and we are committed to having a safe and secure processing environment," the statement said, which added that Heartland was certified as PCI-DSS compliant in April 2008 and "expects to continue to be assessed as PCI-DSS compliant in the future. We're undergoing our 2009 PCI-DSS assessment now, which Heartland believes will be complete no later than May 2009 and will result in Heartland, once again, being assessed as PCI-DSS compliant."

In Richey's E-mail, she also referenced Heartland's comments to Visa that it hopes to be assessed PCI compliant soon. Heartland "will be relisted once it revalidates its PCI DSS compliance using a Qualified Security Assessor and meets other related compliance conditions."

Fines Issued To Banks

Visa also used one of the few other weapons in its PCI arsenal, issuing fines to various Heartland sponsoring banks. Said Richey: "Such fines are part of the program Visa uses to assure compliance with system rules."

Visa also officially "has determined that this event qualifies for the Account Data Compromise Recovery (ADCR) program," which will allow some issuers "to recover a portion of their losses (and it will be) based on a percentage of magnetic stripe-read counterfeit fraud and specified operating expense liability amounts," Richey wrote, giving issuers until May 19 to report those losses to Visa.

The Visa move is interesting, but it appears to be much less about protecting data and card accounts than protecting Visa's public persona. If the suspension prevented Visa transactions from going through Heartland, *that* would have sent a very loud message. But that didn't happen.

What has happened with Visa are some delicious attempts at rewriting history. In presentations that have been given this month by two top Visa data risk executives, Eduardo Perez and Hector Rodriguez, Visa's party line is now "As of today, no compromised entity has been found to be compliant at the time of the breach." And it shall forever be so.

Being Compliant And Being Certified Compliant

Why? Because, as [we've written before](#), there is a huge difference between being PCI compliant and being certified PCI compliant. The differences go way beyond the "one point in time argument" (although that is also a very valid argument). It speaks to the fact that an assessor only knows what he/she is told by the retailer or processor and can only examine what he/she is shown. No assessor is going to ask every possible question, nor envision every possible hole.

As Anthony Freed wrote in his [wonderful analysis of the Visa suspension](#), this is akin to a restaurant inspector. Just because the inspector found the kitchen to be acceptable on Tuesday morning doesn't mean that the chef won't leave the eggs unrefrigerated for five hours later that day. Hence, a good health inspection report certainly does not necessarily mean that it's safe to eat there, just as a PCI certification does not necessarily mean that a retailer is safe to do business with.

Why revisionist history? Because after a major breach, the victim is visited by large teams of Secret Service agents, Visa's top assessors, representatives from their bank and investigators for every lawyer filing a lawsuit against that retailer. I guarantee you that no retailer or processor can undergo that process without someone in that group finding *something*—especially a trivial something—that somehow deviates from a strict interpretation of the PCI rules. And bingo! That retailer or processor is suddenly declared no longer PCI compliant and Visa can say that no PCI compliant entity has ever been breached.

PCI is serious business and this kind of political posturing has a greater potential to undermine payment security—by undermining confidence in the system—than a crew of the best cyber thieves on the planet.