

# Lawsuit: Heartland Knew Data Security Standard was 'Insufficient'

## Complaint Says CEO Described PCI as 'Lowest Common Denominator' of Protection

October 5, 2009 - Linda McGlasson, Managing Editor  
Bank Info Security

Months before announcing the **Heartland Payment Systems** (HPY) data breach, company CEO Robert Carr told industry analysts that the Payment Card Industry Data Security Standard (PCI DSS) was an insufficient protective measure.

This is the contention of a **new master complaint** filed in the class action suit against Heartland, which in January announced a data breach that is now estimated to be the largest known hack, involving 130 million credit and debt card accounts.

In a November 2008 earnings call, according to the complaint, Carr told analysts, "[We] also recognize the need to move beyond the lowest common denominator of data security, currently the PCI DSS standards. We believe it is imperative to move to a higher standard for processing secure transactions, one which we have the ability to implement without waiting for the payments infrastructure to change."

Carr's comment confirms that the PCI standards are minimal, and that the actual industry standard for security is much higher, the complaint alleges. "Heartland executives were well aware before the Data Breach occurred that the bare minimum PCI-DSS standards were insufficient to protect it from an attack by sophisticated hackers," the document says.

Heartland executives have said consistently that the company was PCI-compliant at the time on the breach, which the complaint now says may have begun as early as December 2007. Visa, however, **removed Heartland** from its list of PCI-compliant service providers in March of this year, and one **Visa security executive** was quoted as saying "We have never seen anyone breached that was PCI compliant." Heartland was **re-certified** as PCI compliant in May.

## 1 'Everything We Know About Heartland'

The 52-page master complaint, filed on Sept. 23, is the second of several preliminary legal filings in the class action suit against Heartland on behalf of more than 30 financial institutions from 22 states. Filed in U.S. Southern District Court in Houston, the complaint includes a 10-count claim against Heartland, charging the payment processor with, among other counts:

- breach of contracts;
- negligence;
- violations of the New Jersey Consumer Fraud Act;
- violations of state statutes broadly prohibiting unconscionable acts or practices.

Richard Coffman, of Beaumont, TX, one of the lawyers representing the financial institutions, says the September 23 filing represents "everything we know about the Heartland case so far." The master complaint combines several separate complaints from the attorneys representing the financial institutions in the class action suit.

A **preliminary hearing** in the case was held on August 24 in Houston's Southern District Court of Texas, before Judge Lee H. Rosenthal, who set the dates for future filings in the case.

Heartland now must file its motion to dismiss by October 23. Briefing on the motion will be completed by mid-December. It is anticipated that the motion will be argued in early January.

Meanwhile, as part of the criminal investigation, three individuals have been indicted for the Heartland breach, including alleged ringleader **Albert Gonzalez**.

Also, the **number of institutions** stating publicly that they have been affected by the Heartland breach has grown to 673. This number is estimated by experts to represent approximately one-fifth of all banking institutions affected by the breach.