

# In Legal First, Data-Breach Suit Targets Auditor

- By Kim Zetter [✉](#)
- June 2, 2009 |
- 12:00 am |
- Categories: [Breaches](#), [The Courts](#)



When CardSystems Solutions was hacked in 2004 in one of the largest credit card data breaches at the time, it reached for its security auditor's report.

In theory, CardSystems should have been safe. The industry's primary security standard, known then as CISP, was touted as a sure way to protect data. And CardSystems' auditor, Savvis Inc, had just given them a clean bill of health three months before.

Yet, despite those assurances, 263,000 card numbers were stolen from CardSystems, and nearly 40 million were compromised.

More than four years later, Savvis is being pulled into court in a novel suit that legal experts say could force increased scrutiny on largely self-regulated credit card security practices.

They say the case represents an evolution in data breach litigation and raises increasingly important questions about not only the liability of companies that handle card data but also the liability of third parties that audit and certify the trustworthiness of those companies.

“We’re at a critical juncture where we need to decide . . . whether [network security] auditing is voluntary or will have the force of law behind it,” says Andrea Matwyshyn, a law and business ethics professor at the University of Pennsylvania’s Wharton School who specializes in information security issues. “For companies to be able to rely on audits . . . there needs to be mechanisms developed to hold auditors accountable for the accuracy of their audits.”

The case, which appears to be among the first of its kind against a security auditing firm, highlights flaws in the standards that were established by the financial industry to protect consumer bank data. It also exposes the ineffectiveness of an auditing system that was supposed to guarantee that card processors and other businesses complied with the standards.

Credit card companies have touted the standards and the auditing process as evidence that financial transactions conducted under their purview are secure and trustworthy. Yet Heartland Payment Systems and RBS WorldPay, two processors that recently experienced large breaches, were certified compliant before they were breached. And Hannaford Bros. was certified in February 2008 while an ongoing breach of the company’s system was underway.

A Visa executive [told an audience earlier this month](#) that the companies were not compliant, though auditors certified they were. “No compromised entity has yet been found to be in compliance with [the standards] at the time of the breach,” she said.

In the CardSystems case, Merrick Bank, which is based in Utah and services 125,000 merchants, sued [Savvis](#) last year in Missouri. Merrick says Savvis was negligent in certifying that CardSystems was compliant. The case was moved to Arizona five months ago but only recently assigned a judge, allowing the suit to finally move forward.

According to Merrick’s complaint, in June 2004 Savvis, a managed services company that bills itself as “the network that powers Wall Street,” certified that CardSystems had met the Cardholder Information Security Program (CISP) standards. CISP is the precursor to today’s [Payment Card Industry Data Security Standard \(PCI DSS\)](#).

CISP was developed by Visa, which required card processors and merchants that handled Visa transactions to certify through an auditor that they met a list of standards that included such things as installing firewalls and encrypting data.

Three months after Savvis certified CardSystems, the latter was hacked by intruders who installed a malicious script on its network and stole card numbers. The data belonged to card transactions that CardSystems had retained on its system and stored in unencrypted format, both violations of CISP standards.

The hack, which was discovered only in May 2005, was one of the first that was publicly disclosed under a 2003 California breach notification law. Shortly after the breach became public, VISA [disclosed](#) that CardSystems had not been compliant, even though it passed an audit before the breach. A Visa spokeswoman told Wired at the time that CardSystems had initially failed an audit in 2003, before being certified in 2004, though she wouldn't reveal the reason for the failure.

That earlier audit could become crucial evidence in the case against Savvis, if the plaintiffs can show that Savvis knew about pre-existing problems with CardSystems' security and intentionally overlooked them or failed to ensure they'd been fixed.

According to the complaint, in 2003 CardSystems contracted with a different auditor named Cable and Wireless. Toward the end of that year, the auditor submitted its findings to Visa, which rejected CardSystems's compliance for unspecified reasons. Shortly thereafter, Merrick Bank contracted with CardSystems to process card transactions for its merchant customers, on the condition that the processor achieve certification from Visa.

A second audit was conducted by Savvis, which had bought Cable and Wireless's auditing division. In June 2004, Savvis concluded that CardSystems "had implemented sufficient security solutions and operated in a manner consistent with industry best practices." Visa subsequently certified the processor.

After the hack, it was discovered that CardSystems, which has since filed for bankruptcy, had been improperly storing unencrypted card data for more than five years, something Savvis should have known and reported to Visa. The processor's firewall was also non-compliant with Visa's standards. "Consequently, Savvis' . . . indicating that CardSystems was in full compliance with CISP was false and misleading," the complaint says.

Merrick claims the hack cost it about \$16 million in fraud losses paid to banks that issued the cards, as well as in legal fees and penalties it suffered for contracting with a non-compliant card processor. Merrick says Savvis "owes a duty of care" to audit companies and "breached its duty to competently and professionally assess CardSystems' compliance."

The issue raises questions about the due care placed on certifying certifiers.

PCI auditors are certified by the PCI Security Council, a consortium representing the credit card companies that oversees the PCI standards and certification. According to the Council, about 80 percent of PCI audits are done by a dozen of the largest PCI-certified auditors.

Under the current PCI system, security companies seeking to become auditors must [pay the PCI Council a general fee of between \\$5,000 and \\$20,000](#), depending on the company's location,

plus \$1,250 for each employee engaged in auditing. Auditors are required to undergo annual re-qualification training, which costs \$995.

In light of the recent spate of breaches at companies that were certified compliant, the PCI Council said last year that it was [tightening its oversight of auditors](#).

Previously, only the company being audited was able to view the auditing report, since it was paying for the audit — a situation that mirrors what occurred in the electronic voting machine certification process for years. Now auditors have to submit a copy of the reports to the PCI Council, though the name of the company being audited is redacted.

The Council did not respond to a request for comment, but Bob Russo, general manager of the PCI Security Standards Council, told [CSO magazine last year](#), “We want to make sure no one is rubber-stamping something. We want all these assessors to be doing things with the same rigor.”

The Council said it will also be looking at resumes of people conducting the audits, though it acknowledged that it has only three full-time staff members handling its auditor certification program.

The rules and requirements for auditors reveal [a number of potential conflicts of interest](#) (.pdf) that could arise between an auditor and the entity it’s assessing. For example, many security auditors also make security products. The rules state that a security company will not use its status as auditor to market its products to companies it audits, but if the auditor should happen to find that the client would benefit from its product, it must also tell the client about competing products.

The auditing process isn’t the only problem. Critics say [the standards themselves are too complex](#), and maintaining ongoing compliance is tricky as companies install new programs, change servers and alter their architecture. A company that is certified compliant one month can quickly become non-compliant the next month if they install and configure a new firewall incorrectly.

At a congressional hearing in April to discuss the standards, Rep. Yvette Clarke (D-New York) said that while the standards weren’t worthless, PCI compliance wasn’t enough to keep a company secure. “It is not, and the credit card companies acknowledge that,” she said.

These factors are likely to be part of Savvis’ defense as it fights Merrick’s suit.

Matwyshyn says the case may raise questions about whether an auditor has an ongoing duty to maintain the accuracy of its certification when a company’s security status can change at any time.

“I think it’s not clear as a matter of law to what extent a certification authority has liability in this particular context for a negligent misrepresentation of the security level of an enterprise,” she says.

Matwyshyn says that Merrick's case against Savvis may turn on an Arizona law that allows an entity that is not a direct party to a contract to seek recovery if they are an "intended beneficiary" of the contract. In this case, even though Merrick didn't contract with Savvis directly to certify CardSystems, it relied on that certification being trustworthy.