

# Rare Legal Fight Takes On Credit Card Company Security Standards and Fines

By [Kim Zetter](#), <http://www.wired.com/threatlevel/2012/01/pci-lawsuit/>, January 11, 2012 |



*Photo: Jim Merithew/Wired.com*

A small celebrity-friendly restaurant in Utah is finally doing what many merchants have only dreamed of doing for a long time — taking on a part of the payment card industry’s powerful but flawed system for securing card data by fining merchants for failing to secure their data.

Stephen and Theodora “Cissy” McComb, owners of Cisero’s Ristorante and Nightclub in Park City, Utah, have filed a lawsuit against U.S. Bank claiming that the financial institution, which used to process the restaurant’s credit and debit card transactions, wrongfully seized money from the McCombs’ merchant bank account.

U.S. Bank seized about \$10,000 from the McCombs’ account to pay \$90,000 in fines that Visa and MasterCard imposed after alleging that Cisero’s had failed to secure its network and suffered a data breach that resulted in fraudulent charges on customer bank cards. U.S. Bank sued the McCombs to obtain the remaining balance on the fines, saying a contract the McCombs signed with the bank makes them liable for such fines.

But [in their countersuit against U.S. Bank](#) (.pdf), the McCombs allege that the bank, and the payment card industry (PCI) in general, force merchants to sign one-sided contracts that are based on information that arbitrarily changes without notice, and that they impose random fines on merchants without providing proof of a breach or of fraudulent losses and without allowing merchants a meaningful opportunity to dispute claims before money is seized.

It's the first known case to challenge the heart of the self-regulated PCI security standards — a system that requires businesses accepting credit and debit card payments to implement a series of technological steps to secure data. The controversial system, imposed on merchants by credit card companies like Visa and MasterCard, has been called a “near scam” by a spokesman for the National Retail Federation and others who say it's designed less to secure card data than to profit credit card companies while giving them executive powers of punishment through a mandated compliance system that has no oversight.

“It's just like Visa and MasterCard are governments,” said Stephen Cannon, an attorney representing the McCombs. “Where do they get the authority to execute a system of fines and penalties against merchants? That's a very important issue in this case.”

Legal experts say the case raises a number of broad questions that could have implications for enforcing contracts that many other merchants have signed with banks and card processors.

“All it takes is for one case to drive a truck through a provision of the contract, and all other contracts written like this one are suddenly put into question,” says Andrea Matwyshyn, a law and business ethics professor at the University of Pennsylvania's Wharton School.

Cisero's is a popular Italian eatery frequented by locals as well as celebrities who come to Park City each year for the Sundance Film Festival. Actors Russell Crowe, Sandra Bullock and Sundance founder Robert Redford have all eaten there, [the owners told Bloomberg recently](#).

The issue began for Cisero's in March 2008, when Visa notified U.S. Bank that Cisero's network might have been compromised after cards used at the restaurant were apparently used for fraudulent transactions elsewhere. U.S. Bank, and its Georgia-based affiliate Elavon, process the bank card transactions that customers make at Cisero's.

In the wake of the alleged breach, Cisero's, per rules imposed by the payment card industry, was required to hire a forensic investigations firm — from a list of six firms approved by Visa and MasterCard — to determine if a breach had occurred and if the restaurant was in compliance with the so-called PCI security standards that were adopted by the Payment Card Industry Council in 2005.

The McCombs hired two firms, Cybertrust and Cadence Assurance. Both examined Cisero's point-of-sale system (POS) and servers and found “no concrete evidence that the POS server suffered a security breach which led to the compromise of cardholder data” and no evidence that insiders had installed skimmers on card readers to collect account data. Cadence in fact determined that no evidence existed that payment card data of any kind was improperly taken from Cisero's systems.

The audits, however, did find that the POS system the restaurant used — [a system made by Micros](#) — was storing unencrypted customer account numbers as they were read from the magnetic stripe on bank cards.

Since storage of unencrypted card data is a violation of the [PCI security standards](#), Visa and MasterCard imposed fines on U.S. Bank and Elavon. Under the PCI system, the banks and card processors that process transactions for merchants are fined, not the merchants and retailers themselves. But those banks and card processors have separate agreements with

merchants and retailers that indemnify them against any such fines, forcing the merchants and retailers to pay them instead of the banks and processors — an arrangement that gives merchants little power in challenging fines.

Visa determined that the total cost of the liability for Cisero's noncompliance was \$1.33 million, but ultimately set the fine at \$55,000, without explaining how it reached these figures, the McCombs claim. MasterCard stated that although it could have imposed a fine of up to \$100,000 for the violation of storing card data, it decided to impose a fine of only \$15,000.

The fines increased after card issuers came forward claiming they suffered losses from the alleged breach. Under recovery programs run by Visa and MasterCard, card issuers that have suffered losses due to data breaches can recover these losses from the bank of the merchant accused of being the source of the breach. So after RBS Citizens Bank and Chase claimed they had suffered \$13,849 in losses from fraudulent charges to their customer's accounts as a result of the alleged breach of Cisero's network, MasterCard added that to the fine, for a total of about \$90,000.

But instead of simply notifying the McCombs about the fines and giving them an opportunity to dispute the claims of Visa and MasterCard, U.S. Bank and Elavon simply "helped themselves" to about \$10,000 from the McCombs' U.S. Bank account. The McCombs refused to pay the remainder of the fines and closed their bank account before any more money could be siphoned.

In 2010, Elavon sued to obtain about \$82,600, the remainder of the fines. The McCombs countersued, accusing U.S. Bank of wrongfully seizing their money without providing any proof that a breach occurred or that fraud losses claimed to have been suffered by RBS and Chase were even connected to cards that Cisero's had processed. They accuse Visa and MasterCard of levying "punitive" fines on them that have no relation to actual losses suffered.

To determine the source of a breach, Visa uses a "common point of purchase" method that traces where cards involved in fraud were used in order to find the most likely place where they were stolen. But according to the Cadence forensic report of Cisero's servers, most of the fraudulent activity reported by RBS and Chase involved credit card numbers that were not found on Cisero's point-of-sale system, suggesting they might never have been used at Cisero's. Yet the McCombs were not given a chance to dispute this before the money was seized from their account.

"At no time has Elavon, U.S. Bank, Visa, MasterCard or any other entity proven that a data breach occurred at Cisero's, that issuers actually suffered fraud losses, or that any such losses were caused by a data breach at Cisero's," the McCombs' complaint reads. "Notwithstanding these facts, neither U.S. Bank nor Elavon ever gave Cisero's an opportunity to present evidence in its defense before Visa and MasterCard assessed the fines."

Visa and MasterCard did not immediately respond to a call for comment.

The McCombs also charge that U.S. Bank had a duty to ensure that they were properly notified about the PCI security standards when they were first instituted and had a duty to ensure that Cisero's met those standards. Instead, they say, the standards only went into effect

four years after they signed their contract with U.S. Bank and were incorporated into that contract indirectly, without explicit notice of the new rules. The McCombs say the bank only made reference to the rules via a web site address that appeared on six printed bank statements sent to the McCombs between 2005 and 2007. Since the McCombs did their banking online, they never noticed the reference and only learned of the rules when they were told they might have violated them.

The McCombs assert that the PCI system is less a system for securing customer card data than a system for raking in profits for the card companies via fines and penalties. Visa and MasterCard impose fines on merchants even when there is no fraud loss at all, simply because the fines “are profitable to them,” the McCombs say.

Furthermore, there is no recourse and no process available for merchants to challenge fines, they say in their complaint. Although the acquiring bank, such as U.S. Bank, can appeal the fines in writing with supporting material, the banks have no incentive to do so, since they are indemnified from liability in their contracts with merchants and simply pass the fines onto the merchants. Banks also have to pay a nonrefundable fee of \$5,000 to file an appeal, giving them even less reason to do so.

Matwyshyn says the system of fining merchants could prove to be a problem for the payment card industry if the court views them as punitive in this case.

“In general, contract law does not like punitive damages being included in contracts,” she says. “If you argue that these fines are punitive and unrelated to actual losses suffered, courts could deem your contract to be overreaching and conclude that its intent is to punish rather than to compensate harm.”

Matwyshyn also says the fact that merchants are liable for a third-party agreement their banks make with Visa and MasterCard is also problematic because it disempowers merchants and prevents them from being able to “negotiate the kinds of balanced provisions we would expect to see between two parties to a contract.”

“We should see some interesting contract analysis from the court [on this],” she said.

*Photo: Jim Merithew / Wired.com*