Radiant Being Sued by Restaurants for violating PCI Compliance

By Administrator on December 3, 2009 2:58 PM

Radiant being sued not over it's Aloha system which is PCI-validated but over the use of PC Anywhere.

Restaurants Sue Vendor for Unsecured Card Processor

- By Kim Zetter ✉
- November 30, 2009 |
- 11:44 pm |
- Categories: Breaches, The Courts
-

Seven restaurants have sued the maker of a bank card-processing system for failing to secure the product from a Romanian hacker who breached their systems.

The restaurants, located in Louisiana and Mississippi, filed a class-action suit against Georgia-based Radiant Systems for producing a point-of-sale (POS) system that they say was not compliant with payment card industry security standards and resulted in an undetermined number of customers having their debit and credit card numbers stolen.

The suit alleges that the system stored all the data embedded on the bank card magnetic stripe after the transaction was completed -- a violation of industry security standards that made it a high-risk target for hackers.

Also named in the suit is Computer World, a Louisiana-based retailer, which sold and maintained Radiant's Aloha POS system.

According to plaintiffs, Computer World's technicians allegedly installed the remote-access program PCAnywhere on the systems to allow its technicians to fix technical problems from off-site. The only problem is, the company failed to secure the program. The suit alleges that the system was not up to date with software patches, and the PCAnywhere remote log-in and password that technicians used to access the POS systems was the same at every one of the 200 Louisiana locations where the system was installed. According to one of the plaintiffs who spoke with Threat Level, the default login was "administrator" and the password was "computer."

As a result, a hacker, believed to be based in Romania, accessed the systems of at least 19 businesses through the PCAnywhere software, and possibly others plaintiffs say. Once inside, the hacker installed malware to grab card data as it was swiped and send it to an e-mail address in Romania. The hack follows a wave of similar attacks that targeted point-of-sale systems at other national retailers and restaurant chains between 2005 and early 2009, including Dave & Busters restaurants, Hannaford Brothers, TJX, Wal-Mart and others.

The suit was filed in March in the U.S. District Court in Louisiana, but the court ruled only last week that the seven plaintiffs could proceed as a group with their case, opening the way for additional plaintiffs to join the litigation.

"We want other restaurants nationally to be aware of the hidden dangers posed by these technology companies and the unfair penalties imposed by the credit card companies," said plaintiffs attorney Shiel Gallagher in a press release. "These huge companies shouldn't have the power to destroy these restaurants."

The plaintiffs include Crawfish Town USA, Don's Seafood & Steak House, Jone's Creek Cafe, Mel's Diner, Picante's Mexican Restaurant, Sammy's Grill and a Best Western. Two other restaurants have also sued Radiant Systems and Computer World separately.

The restaurants are seeking millions in damages to recover their costs from the breach. These include fines levied against them from Visa and other credit card companies for failing to be PCI-compliant, the cost of forensic audits to uncover the source of the breach, chargebacks to cover fraudulent charges made on customer accounts and reimbursements to card providers who had to issue new customer cards.

According to the plaintiffs' court filing (.pdf), Radiant and Computer World were allegedly warned by Visa in April 2007 that the Aloha system, along with POS systems made by five other vendors, were non-compliant because they stored card data. Visa also sent out a bulletin in November 2006 warning that one of the most frequent vectors for hackers to penetrate POS systems was through poorly configured or unpatched remote-access software (.pdf) and default passwords. Nonetheless, the restaurants say, Radiant and Computer World sold them a product that was neither PCI-compliant nor secured against a known attack.

PCI compliance involves 12 requirements that include: installing and maintaining a firewall, changing default vendor passwords, encryption of transaction data while it's being processed and updated security patches and anti-virus definitions, among other things. Businesses that accept bank card payments from customers are contractually required by the payment card industry to have PCI-compliant architectures and to use only products that are PCI-compliant.

Charles Hoff, general counsel for the Georgia Restaurant Association and one of the plaintiffs' attorneys, says these kinds of security disputes are becoming more common but rarely garner public attention because vendors tend to settle rather than risk exposure through a court case. He said this suit was filed only after Radiant refused to take responsibility for the breaches.

"Radiant ... took a very arrogant attitude about it," he told Threat Level. "I've had other POS vendors who felt they should be accountable, and the end result was that they knew they needed to do the right thing. Radiant I don't think thought we were serious. Radiant's website gives customers the greatest assurance that when it comes to their resellers, they monitor and make sure they're scrutinized and compliant. It really would give you all the confidence in the world if it was actually done."

Radiant has declined to comment on the details of the suit.

"What we can say is that Radiant takes data security very seriously and that our products are among the most secure in the industry," Paul Langenbahn, president of Radiant's hospitality division, told the *Atlanta Journal Constitution*. "We believe the allegations against Radiant are without merit, and we intend to vigorously defend ourselves."

Keith Bond, owner of Mel's Diner in Broussard, Louisiana, told Threat Level that he purchased his Aloha system for $20,000 and installed it around late November 2007. Computer World, he says, convinced him that the system needed to be connected to the internet for faster transaction processing, as opposed to the dial-up modem connection he had been using for processing.

In April 2008, just a few months after installing the system, one of his employees called to tell him that the mouse cursor on one of three Aloha terminals he'd bought seemed to be moving on its own and that employees were unable to take control of it.

After contacting Computer World technicians, the restaurant was told to disconnect its system from the internet. A service tech appeared the next day to replace the hard drive, but didn't disclose the nature of the problem or indicate that an intruder had breached the system. Bond learned only later that a keystroke logger had been installed on all three of his Aloha terminals, and that the intruder had been siphoning card numbers for about three weeks.

He discovered this only after Visa and Mastercard contacted him in May to tell him his system had been breached. Bond, whose 24-hour diner processes about 60 to 70 card transactions a day, says 669 card numbers were stolen during the three-week period the hacker was in his system.

"If they had accessed the server, they would have got thousands of card numbers," Bond said.

The credit card companies forced him to hire a forensic team to investigate the breach, which cost him $19,000. Visa then fined his business $5,000 after the forensic investigators found that the Radiant Aloha system was non-compliant. MasterCard levied a $100,000 fine against his restaurant, but opted to waive the fine, due to the circumstances.

Then the chargebacks started arriving. Bond says the thieves racked up $30,000 on 19 card accounts. He had to pay $20,000 and managed to get the remainder dropped. In total, the breach has cost him about $50,000, and he says his fellow plaintiffs have borne similar costs.

Bond said Radiant and Computer World were unresponsive.

"Radiant just basically hung us out to dry," he says. "It's quite obvious to me that they're at fault.... When you buy a system for $20,000, you feel like you're getting a state-of-the-art sytem. Then three to four months after I bought the system, I'm hacked into."

Image courtesy California State Controller's Office