

Bank Information Security Articles

POS System Breached?

Fla. Restaurant Investigated After \$200,000 Fraud Spree

September 27, 2010 - Linda McGlasson, Managing Editor



A summertime spike in credit card fraud in the Tallahassee, Fla., region is linked to one restaurant that had its point of sale software targeted by hackers, resulting in \$200,000 in fraud losses.

Julie's Place, a Tallahassee eatery, was identified by the [Leon County Sheriff's Office](#) Financial Crimes Unit as the source of the card compromises, which involve more than 100 consumer accounts. This incident is only one of several [payment card crimes](#) reported in Florida this summer.

The twist in this case: The hackers targeted the data somewhere between the network and the restaurant's processor. This breach has prompted the major credit card companies to request a full forensic investigation of the incident. Meanwhile, the manufacturer of the payment software says its system was not the cause of breach.

POS Breach

Julie's Place owner Dave Wendland says he began hearing about the credit fraud from customers in July. Several patrons told him that fraudulent, out-of-state credit card charges were appearing on their cards. Wendland subsequently called his point of sale vendor and his acquiring bank to check the security of the system. The sheriff's office contacted the restaurant shortly afterward and began its investigation. In all, fraudulent charges of more than \$200,000 have been reported on more than 100 credit cards used by Julie's Place customers. The restaurant has accepted credit cards since opening in 1978.

Wendland says investigators believe the breach occurred on transactions somewhere between the restaurant's POS terminal and the processor, located in Washington state. The company that provided the Aloha card terminal also found evidence, Wendland says, that the intruder got past the POS system's firewall and was able to remotely steal the customers' information. The technician's evaluation showed malware that was specifically for the Aloha system used by the restaurant.

Visa and MasterCard have requested that Julie's Place do further forensics into the event. Wendland says that Trustwave, a Chicago-based computer forensic firm, has started reconstructing the hard drive involved in the attack to determine what happened. The final cause hasn't been determined yet.

As recently as a year ago, Wendland says the POS vendor had a PCI assessment done of the equipment and network, and it was found to be compliant.

Radiant Systems, the Atlanta-based point of sale vendor that developed Aloha systems, says its software was not breached. Ernie Floyd, director of data security and compliance, says what has happened to Julie's Place isn't uncommon - the restaurant's system was breached because it didn't meet PCI requirements.

Floyd says his sources have informed him that the restaurant had insufficient firewalls installed, and the network had its remote access running in "open" mode, meaning that someone with the right tools would be able to access the network and everything that wasn't protected. As for the claim by Julie's Place owner that the restaurant was found to be PCI compliant, Floyd says "This merchant may have upgraded to a PA-DSS validated system, but they didn't do anything further to lock down its security."

Wendland says the restaurant now has replaced the entire POS with new terminals and updated network software. "Our POS system is completely 'locked down' now," he says.

Merchants Are Targeted

Banking institutions should let their business customers know: There is malware being directed at small businesses, including restaurants, according to Colin Sheppard, director of incident response for Trustwave. While Sheppard cannot comment on the ongoing investigation at Julie's Place, he does confirm that such malware attacks are happening. Criminals aren't able to find card data stored on systems any longer because most retailers are no longer saving it. "So now the hackers have moved to capture the data while it is in transit," Sheppard says.

The three main types of malware attacks Trustwave is seeing:

- **Network Sniffers** - capturing data while it is going over the wire;
- **Keyloggers** - capturing data at the card swipe;
- **RAM scrapers** - which takes the data by scraping it right out of the RAM.

Of these three types, Sheppard says keyloggers are on an uptick in the investigations Trustwave has done in the past year. And RAM scrapers, also known as memory dumping, is "very popular."

The malware problem has always been out there, but Sheppard notes that food and beverage retailers, including restaurants, are the "low hanging fruit" for hackers, who can use "cookie-cutter" attacks against them because many of these retailers have the same point of sale systems.

That Aloha's POS software was specifically targeted troubles Branden Williams, director of the Security Consulting Practice at RSA, the security division of EMC. He says it's always been a question in his mind when this type of software would be targeted. There was one "proof of concept" piece of malware written for another vendor's point of sale software recently, he says.

"The proof of concept malware was to show that just putting AV on the network didn't stop the problem," he says. At the POS level, Aloha and MICROS, the two largest vendors in the market, will continue to be the software hackers will target, Williams says. Sheppard adds that the kind of malware targeting the two largest vendor POS systems will easily work on smaller vendors' products, too, so no one is safe.

The Best Defense

Both Sheppard and Williams intone a "back to the basics" approach for merchants in constructing a better secured network for card transactions. Both also remind retailers and other businesses that the PCI requirements are the basis, but not the end, of a security program. "It is a cliché, but security is an ongoing, 24X7 process," Sheppard says.

They're tips for banking institutions to share with business customers:

- **Use PCI-Validated POS Equipment** - This will mean an upgrade for many small retailers. There are newer tamper-proof options from vendors, says Dave Shackelford, a security expert at Sword & Shield, a computer and network security firm in Atlanta, but many small retailers are still using older equipment.
- **Install a firewall** - and make sure it is configured correctly.
- **Get Anti-Virus** -- have it installed on every machine and keep all signatures up to date.
- **Log Everything on the Network** - Store log data, and regularly have someone who knows how to look at it check it for aberrant traffic.
- **Patch Your Systems** - check for patches and sign up for automated patches where possible.

Learn About the Risks - Don't depend on your third-party vendors or processors to tell you that everything is okay. Also, be sure to ask your vendor about proper configuration of point of sale systems - get the guarantee in writing.