

Advertisement



Powered by Clickability

Click to Print

[SAVE THIS](#) | [EMAIL THIS](#) | [Close](#)

Thieves skim credit card data at fuel pumps

By Katharine Lackey, USA TODAY

Customers and police agencies across the USA are dealing with another pain at the pump — thieves who install hard-to-detect electronic devices at stations to steal credit and debit card data.

The skimmed data are used to create cards used at the victims' expense, says James Van Dyke, president and founder of Javelin Strategy and Research, a financial consulting firm that focuses on fraud and identity theft.

STORY: [Meet A-Z, the computer hacker behind a cybercrime wave](#)

Investigations of theft related to skimming devices at gas pumps continue in California, Washington, Nevada, Pennsylvania and Delaware, according to various police departments.

Though the most recent cases don't necessarily represent an epidemic, the Secret Service is investigating incidents across the country, says Ed Donovan, spokesman for the agency, which has financial and electronic crimes units.

Skimming devices have been used for several years, most often at ATMs. Thieves increasingly target pumps because it's a cheap, easy way to steal credit and debit card information, Van Dyke says.

"Card fraud at gas pumps is a significant problem, and that's because of the unintended nature of the checkout devices," he says. "Essentially, every gas pump is an electronic cash register."

The skimming devices can be installed outside or inside the pump. Thieves glue a plastic sleeve, equipped with covered wires that capture data, over the pump's card reader or connect the device directly to the reader inside.

The devices are molded and painted to match the machine and are small, making them hard to detect, Van Dyke says. Among recent cases:

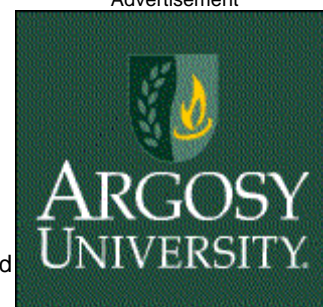
• **California:** San Jose police are investigating a case that began in May, when thieves placed a skimming device at an Arco station, eventually taking more than \$200,000 from up to 180 victims, says police department spokesman Jermaine Thomas. The device was on the pump for more than a month, after which the suspects retrieved the machine, Thomas says.

"Your normal, average person would not even know that the skimming device is attached," he says.

• **Washington:** The Pierce County Sheriff's Office is investigating a case where thieves installed a skimming device at an Arco gas pump last August, leaving it there for 11 months and cleaning out at least 120 victims' bank accounts over the July 4th weekend, says sheriff's spokesman Ed Troyer.

Reports of fraudulent withdrawals are still pouring in, and the number of victims could reach 250 with a total of \$500,000 stolen, he says.

Advertisement



On Campus, Online

practitioner-focused
psychology and
counseling degrees[Click To Learn More ▶](#)

• **Pennsylvania:** State police recovered four skimming devices installed inside gas pumps at Wawa stations in Delaware, Chester, Montgomery and Bucks counties beginning in April, trooper Christopher Shoap says. He suspects more devices were used at other stations and estimates that several dozen victims have lost tens of thousands of dollars.

• **Delaware:** The Pennsylvania case is linked to one in Delaware, where police suspect a device was placed and later retrieved at a New Castle Wawa pump, Shoap says. The Secret Service is investigating, says Cpl. Jeff Whitmarsh of the Delaware State Police. The Secret Service would not comment because the investigation is continuing.

• **Nevada:** The Las Vegas Metropolitan Police Department is investigating two devices placed at gasoline pumps within the past four months, in addition to several cases where devices were placed on ATMs, says Lt. Bob Sebby of the financial crimes unit.

The combined cases total \$1 million to \$3.5 million stolen from hundreds of victims' accounts, Sebby says. The department is trying to prevent additional identity fraud by asking gas stations to consider placing sticker seals on the pumps that employees can check daily.

"With identify theft, it's not a matter of if you're going to be a victim, it's a matter of when," Sebby says.

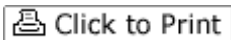
Links referenced within this article

Meet A-Z, the computer hacker behind a cybercrime wave

http://www.usatoday.com/tech/news/computersecurity/2008-08-04-hacker-cybercrime-zeus-identity-theft_N.htm

Find this article at:

http://www.usatoday.com/money/industries/energy/2008-08-04-gaspumpskimming_N.htm



[SAVE THIS](#) | [EMAIL THIS](#) | [Close](#)

Uncheck the box to remove the list of links referenced in the article.

Copyright 2008 USA TODAY, a division of Gannett Co. Inc.