THE WALL STREET JOURNAL.



http://www.wsj.com/articles/credit-card-fraudsters-pump-gas-stations-for-profit-1441253132

MARKETS

# Credit-Card Fraudsters Pump Gas Stations for Profit

Payment-card companies and gas-station operators combat a wave of theft

A delay in guidelines encouraging gas stations to upgrade their equipment leaves them more vulnerable to credit-card fraud than other sectors. *PHOTO: DAVID PAUL MORRIS/BLOOMBERG NEWS*

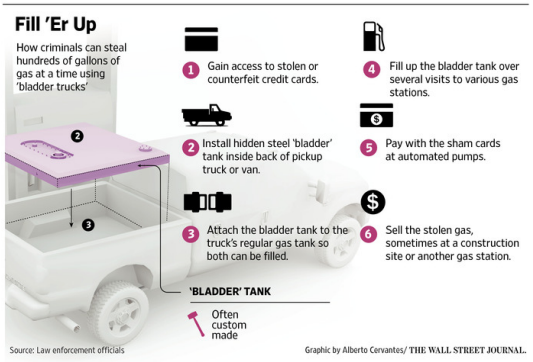
By **ROBIN SIDEL**

Updated Sept. 3, 2015 12:55 p.m. ET

Credit-card fraudsters are filling up at the gas pump.

As motorists head out on the last big driving weekend of the summer, the credit-card industry and gas-station owners are deploying everything from sophisticated software to heavy-duty padlocks to combat an epidemic of fuel-related theft and fraud.

The crackdown is gaining additional momentum because many gas stations will be among the last merchants to install equipment accepting a new generation of fraud-resistant cards. While many big merchants will have equipment in place by Oct. 1 to accept the new chip-based cards, tougher guidelines set by Visa Inc. and MasterCard Inc. don't apply to gas stations until 2017.




That delay could exacerbate what analysts, card companies and law-enforcement officials say has been a recent surge in fraud at the pump.

"The concern is that this is still a gaping hole that has not been well addressed and now there are conditions that are going to make it worse," says Al Pascual, a director of fraud and security at Javelin Strategy & Research, a unit of

Greenwich Associates LLC.

The crime wave has been driven by the flood of stolen credit-card data easily accessible online, much of which was swiped in high-profile breaches. Last year alone, popular retailers Home Depot Inc., Staples Inc. and Supervalu Inc. were hit by hackers. Stolen numbers are available for as little as 50 cents apiece, experts say.

Gas stations make easy targets for those who want to make fraudulent purchases using stolen numbers, since pumps are usually unattended.

In addition, law-enforcement officials say it is increasingly common for crooks to rig pumps with "skimming" devices, which capture data from the magnetic strip on customers' cards. Thieves can use that data to create counterfeit cards.

In May, Florida state officials conducted a series of sweeps that found more than 100 skimmers at gas stations.

In recent weeks, law-enforcement officials in California for the first time found devices that skim card data from unsuspecting gas-station customers and then relay the information to crooks via text message, says Steven Scarince, a U.S. Secret Service agent in Los Angeles who runs a task force that specializes in gas-pump-skimming investigations.

RELATED

- Small Businesses Are Slow to Embrace New Chip-Card System (http://www.wsj.com/articles/small-businesses-are-slow-to-embrace-new-chip-card-system-1441239109)

"Their technology keeps improving year after year," he said. "Boy, are we busy."

Credit and debit cards account for more than half of all U.S. gasoline purchases, according to Nilson Report, a Carpinteria, Calif.-based newsletter that tracks the payments industry.

Gas stations also are being hit by criminals who use counterfeit cards to fill up tanks hidden inside vehicles called "bladder trucks" that can hold hundreds of gallons of gas. The criminals then sell the stolen fuel to unscrupulous gas-station owners or construction sites.

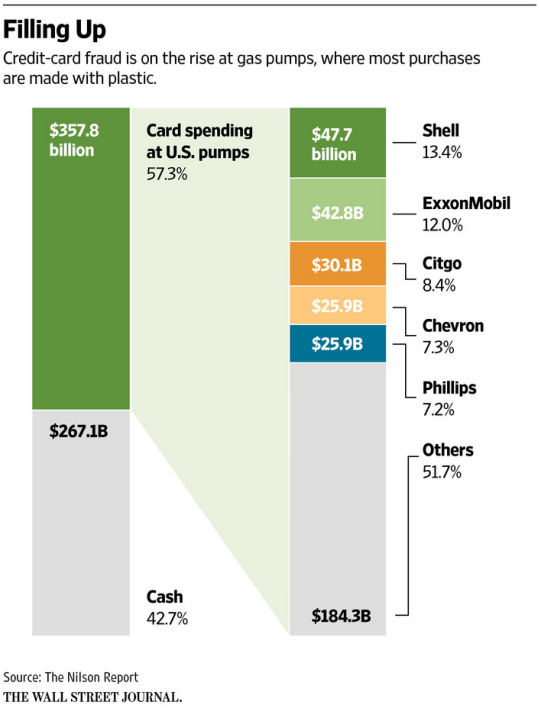
"It's frustrating how many times it's happening. We spend a lot of time chasing it and trying to prevent it," says Brian Decker, operations manager for SC Fuels, an Orange, Calif.-based distributor that also operates retail gas pumps.

In June, a Tampa. Fla., man was arrested and accused of using eight counterfeit cards to buy hundreds of gallons of fuel. The 27-year-old suspect used a bladder truck that was retrofitted with a custom-made steel tank hidden under the cover of his pickup-truck bed.

It is difficult to pinpoint the amount of gas-station fraud, in part because the losses are spread among station owners, card-issuing banks and consumers who often don't realize their card data was stolen. The gas-station industry estimates it incurred losses of $250 million in 2013, the most recent year for which information is available, while the payment-card industry estimates it lost $500 million on fuel-related fraud that year.

Card-issuing banks pick up the cost of fraudulent transactions tied to counterfeit cards made from stolen numbers, but the gas stations are on the hook if the physical card being used has been lost or stolen.

Last year, Visa introduced a new fraud-detection system specifically for gas stations that attempts to cut down on counterfeit transactions by determining whether the person using a debit card or credit card is the true owner of the plastic. Customers whose cards trip certain risk factors are asked to complete the transactions inside the station, rather than at the unattended pump.




Among the possible warnings signs are if a card has been used in two distant locations within a short period, or if the card has been used to fill up multiple times recently.

Visa says that its fraud-prevention program is being used at roughly 30,000 gas stations, or 20% of the U.S. total. Fraud-related losses are down 23% at Chevron Corp. gas stations that began using Visa's technology in February 2014, says Gabriel Andres Porras, merchant-acquiring manager at the oil giant.

MasterCard began rolling out similar technology last month.

The new chip cards being rolled out aren't yet expected to be an added defense against fraud at most stations. These cards issue a unique code for each transaction, making them more difficult to counterfeit than traditional cards with a magnetic strip.

Starting on Oct. 1, merchants will bear the cost of fraud that occurs if a customer pays with a chip card but the merchant doesn't have technology to process a chip-based transaction. As of now, the financial institution that issues the card is on the hook to for fraud. But because station owners won't face greater liability until 2017, many aren't expected to upgrade their pumps until then, partly because it costs several thousand dollars per dispenser to do so.

"One of our fears is that we know it's going to take a long time to upgrade their pumps," says Mark Nelsen, senior vice president of risk products and business intelligence at Visa.

The card companies say gas stations were given more time to comply because automated fuel dispensers are more complicated to upgrade.

Gas-station owners, meanwhile, are trying to fight the increase in fraud by putting padlocks and special seals on fuel dispensers to prevent thieves from tampering with the pumps and installing skimmers.

Such efforts are coming too late for Gregg Laskoski of Spring Hill, Fla., whose bank alerted him in March to a fraudulent purchase of gasoline on his debit card in a town about 25 miles away, even though he never lost possession of his card. The purchase was for $125 worth of fuel—more than what his small car could handle.

"I'm a little more leery about any type of transactions that aren't cash, but there's a great deal of convenience with a debit card," says Mr. Laskoski. His bank replaced the money taken from his account after verifying that the transaction wasn't his.

**Corrections & Amplifications:**
Mark Nelsen is senior vice president of risk products and business intelligence at Visa. An earlier version of this article misspelled his surname. (Sept. 3, 2015)

**Write to** Robin Sidel at robin.sidel@wsj.com