PAYING FOR GAS AT THE PUMP

Scammers are targeting gas stations with increasing frequency. Here's how you can protect yourself from fraud.

It’s a simple fact of daily life: If you drive a car, you need to fill it up with gas regularly. But this part of your everyday routine could be putting you—and your bank account—at serious risk. Credit-card fraud at gas stations is rising significantly, prompting banks, law-enforcement agencies, and credit-card companies to urge consumers to avoid paying at the pump and instead pay inside whenever possible. Here’s what you need to know.

The most common scam tool

Gas-station fraud commonly occurs with the use of skimmers—small devices that thieves place on or above the card readers at gas pumps (and also ATMs) to copy and steal your card information. How big is this problem? In 2018, Florida investigators found nearly 1,000 skimmers at gas pumps in that state alone. And according to data from the credit-scoring company FICO, fraud from card skimming is increasing nationally at the rate of 10 percent per year.

According to Robert Siciliano, a security expert for Porch.com, gas-pump skimming can happen in a number of different ways. “Criminals can install a skimming device on the face of the pump where users insert their card, or they will get access and purchase pump keys online to open up the actual pump itself and insert an internal skimmer in line with the point-of-sale (POS) Internet connection,” he explains. These skimmers are even customized to the gas pump or ATM machine to which they are affixed. “In other words, the plastics are shaped, colored, and molded specifically to the device in which they are attached,” Siciliano says. “It is very difficult for a consumer to determine what is real and what is fake, or if there is a device attached to the face of their ATM or gas pump.”

One Secret Service agent who was involved in an investigation about gas skimmers was the victim of gas-pump fraud himself—twice. So, even a government official who’s trained on this topic often can’t tell if skimmers are there. Siciliano adds that it’s becoming increasingly common for gas pumps to be skimmed internally: “This means there is a device attached in the communication lines that intercepts the card number as it travels over the Internet.”

Look for signs of tampering

If a crook has opened up the pump itself to place the skimmer or other device inside, that's even tougher to detect, but there may be a clue. "One way to spot a pump that's been tampered with is to look for security seals that are properly placed," says Greg Mahnken, a credit industry analyst at Credit Card Insider. "Employees will usually place security seals over points of entry for the pump, such as over a keyhole or where the pump swings open for service access. Security seals are tamper-evident."

According to the FTC, these seals are large adhesive labels that are generally placed on the pump, near the card reader. If they've been tampered with—i.e., the seal has been broken or the sticker has been removed—you'll see text that you won't see otherwise. "Most security seals will read the word VOID if they've been peeled, stretched, or otherwise tampered with," says Mahnken. "If you see a security seal that reads VOID, don't use that pump and notify an employee."

Scammers are getting more sophisticated in their tactics

While we generally think about card skimmers when we talk about gas-station security risks, there are new high-tech scams that involve other tactics, some of which don't require the scammer to physically go to that location at all. In November 2019, Visa issued a security alert about two attacks in which someone sent a malware-infected phishing email to a merchant employee, which allowed the scammer to access the POS payment processing system for those who paid at the pump. This is another reason why you should always pay inside, if you can. Bonus: While you're in there, you can caffeinate yourself. Know where to stop by checking out this map of the best gas station coffee in every state.

Chip cards offer enhanced security

So, how can you protect yourself? According to Visa, "non-fuel merchants that are chip-enabled have experienced a significant 81 percent decrease in counterfeit fraud dollars." However, troubling statistics show that only 10 percent of fuel pumps nationwide have this feature. Visa recommends that "consumers should remember to check the fuel pump to see if a chip reader is installed. If they are not sure if the pump is safe, pay inside with a chip card."

Payment stations usually indicate if they have a chip reader. But you can also tell because you need to keep your card inserted while the system reads the chip, as opposed to just quickly sliding the card in and out, as you do for old-fashioned magnetic stripe readers.

Gas merchants have been much slower to incorporate EMV (chip reader) technology than retail stores, but this tech will eventually be more widespread. “The fuel segment has its own unique challenges, which we recognized when we first set the chip activation date for automated fuel dispensers/pumps (AFDs) two years after regular in-store locations,” noted an official Visa statement. While that EMV activation date for gas stations has been pushed back, it is on the horizon: October 1, 2020.

Debit cards put you at the greatest risk

While any form of plastic payment can be stolen or compromised, debit cards present the most risk because if thieves get your card information, they can quickly drain your account or leave you without access to your money. Most debit cards also generally don’t have the same protections as credit cards, though Visa notes that its Zero Liability Policy protects cardholders against fraud and unauthorized charges for both debit and credit cards equally. Still, experts recommend that it’s usually best to use a credit card and, ideally, pay inside. Or if you use the same gas stations frequently, buy gas-station gift cards. They don’t have any of your personal information connected to them, and since they have a limited value, your potential losses—should a scammer somehow get the numbers—would be relatively minimal.

Take advantage of your card’s fraud-prevention features

Most credit-card companies now offer an array of safety features that help you avoid getting scammed or allow you to react quickly in case of fraud. Visa urges cardholders to explore the range of transaction controls and alerts that mobile apps can offer cardholders—such as the ability to freeze/disable their card, set controls as to the type of purchases/merchants allowed, and set up alerts for purchases and transactions.