



Your Monthly Money

brought to you by



7 Ways to Avoid Getting “Skimmed” at the Gas Pump

Take these steps to foil criminals after your credit or debit card data when you fill up.

The national average gas price was \$4.77 a gallon as of the first week of July, according to AAA. Depending on how big your vehicle’s gas tank is, you’re already paying what may seem like a fortune at the pump. But what if you had to pay even more, straight from your bank account or credit card, thanks to criminals attaching credit and debit card skimmers to the payment terminal?

Skimming can happen if you pay with a credit or debit card at a gas pump that has an illegal Skimming skimmer, a card reader that steals data from your card’s magnetic strip. Gas pump pay terminals aren’t the only place you may encounter a skimmer, either. Criminals also attach card skimmers to ATMs and other types of point-of-sale (POS) terminals, too.

Skimmers at gas pumps, ATMs, and POS terminals cost consumers and financial institutions more than \$1 billion each year, according to the FBI.

Once thieves steal your card’s data, they either sell the stolen data to other criminals or use your credit card number to make fraudulent purchases. If you don’t check your bank or credit card account regularly, you probably won’t even know that your card number has been stolen or used for fraudulent transactions.

Worried you could become a skimmer’s next target?

Below are seven ways to help protect your credit or debit card data from criminals eager to swipe those numbers when you use your card to fill the tank.

1. INSPECT THE FUEL PAYMENT PANEL

It’s easy to miss signs that a card skimmer is waiting to steal your data. That’s because skimmers are often (but not always) attached to the wiring inside the pump, according to the FBI. That doesn’t mean won’t see signs of tampering if the skimmer is attached outside, though.

For example, many gas stations place a security seal that looks like a piece of tape over the payment panel. If someone has opened the panel to install a card reader in the wiring, the tape will display “void,” according to the Federal Trade Commission (FTC).

2. LOOK CLOSELY AT THE CARD READER

Before you swipe your card at the pump, take a minute to compare the card reader to the ones on the other gas pumps. Is it identical, or does it look different in some way? Maybe it sticks out further than the rest, for example.

The FTC recommends trying to wiggle the card reader before using it. “If it moves, report it to the attendant,” advises the FTC. “Then use a different pump.” Even with these measures, however, you won’t be able to detect an internal card skimmer.

3. USE THE CHIP READER INSTEAD

When you insert your credit or debit card into the chip reader, your credit card number is more secure from being skimmed. “In the U.S., there are fewer devices that steal chip data vs. magnetic strip data,” according to the FBI.

But even this method may not protect your card’s data. That’s because when you insert a chip card, you could become a victim of “shimming,” where criminals insert a thin device called a shim into the card reader where you insert your chip-enabled card to clone the data on the magnetic strip.

At this point, shimming can’t clone the three-digit CVV security code on the back of the card, so criminals may find it more difficult to use your card to make fraudulent purchases, according to major credit bureau Experian.

4. USE A PUMP NEAR THE ENTRANCE

When choosing a gas pump, use one that’s close to the gas station entrance rather than one toward the back of the lot. “Choose a fuel pump that is closer to the store and in direct view of the attendant,” advises the FBI. “These pumps are less likely to be targets for skimmers.”

5. PAY WITH A CREDIT CARD

If you pay for gas with a credit card and the card’s data is stolen for fraudulent transactions, federal law limits your liability to \$50. Most credit card companies go further with a zero-liability policy when the card is used for fraud.

When you pay with a debit card, you won't have that same liability protection, and fraudulent purchases with the debit card are deducted directly from your checking account. Even worse, if someone gains access to the PIN you enter, they also have access to your cash.

6. PAY WITH MOBILE WALLETS

If it's an option, pay with mobile payment options such as Google Pay, Apple pay or similar mobile wallets, advises Experian. That way, your credit or debit card gets nowhere near a card skimmer.

7. PAY INSIDE

We all love the convenience of paying with a credit card at the pump. But if you don't want to risk unwittingly handing over credit or debit card numbers to criminals via a card skimmer, the best protection is to trudge up to the station door, wait in line and pay the cashier.

While there is less chance that someone installed a skimmer or shim to the POS terminal inside, there's still some risk when you use your card. The only foolproof way to not get shimmed or skimmed is to pay cash (or using a mobile payment system) when you fill the tank.

For more financial education information visit your [KOFE Portal!](#)