Credit card fraud is a concern for all Americans, and with the introduction of EMV chip cards, **counterfeit fraud at U.S. retailers has seen a decline** [2]. Despite the efforts of the major credit card companies and their EMV chip requirements, fraud has continued to rise as a whole, specifically at the gas pump. While the deadline for retail merchants to make the change to EMV enabled equipment or face a shift in liability has passed, both **VISA** [3] and **Mastercard** [4] have given Automated Fuel Dispensers an extended deadline stretching until 2020.

According to the **Identity Theft Resource Center** [5], hacking, including phishing, ransomware/malware and skimming, was the leading cause of data breaches in the first half of 2017.

While phishing and ransomware present problems, skimming is the primary concern at the pump.

“Skimming typically requires two devices to be installed. ...[O]ne piece skims, or captures, the data from a card’s magnetic stripe, while an accompanying pinhole camera captures cardholders’ PINs as they’re entered,” according to the **FBI** [6]’s website.

These devices are normally undetectable by distracted or rushed consumers in their haste to fill up. Skimmers usually blend in with the gas pump’s façade and appear to be legitimate.

From California to Florida, personal credit card information is being stolen at the pump, and in at least one instance, the fraud has prompted federal law enforcement investigations and crackdowns.

In a November 2017 **press release** [7], the Department of Justice, U.S. Attorney’s Office for the Western District of Kentucky, disclosed that an investigation estimated the presence of up to 50 active skimmers in the greater Louisville area and a financial loss of more than $3.5 million from six cases combined where over 7,000 unique card numbers had been affected.

There are **actions** [8] concerned motorists can take before swiping his or her card at the pump:

1. Make sure there are no signs of tampering – check security seals, cabinet panels, etc.
2. Try to wiggle the card reader - it should be secure.
3. If using a debit card, run it as credit to safeguard the PIN.
4. Monitor credit card and bank accounts to catch unauthorized charges.
5. Pay in-store instead of at the pump.

States have been taking actions to combat skimming. Several states have been using their departments responsible for weights and measures inspections to lock for skimmers when doing compliance checks. Unfortunately for Americans, these efforts can only do so much.

For obvious reasons, each pump cannot be inspected every day. Inspectors check all the pumps in their respective states, and pumps are generally only inspected once per year. Although protocols do exist in many states to report a suspect pump, this leaves ample opportunity for criminals to gain the
sensitive information they seek.

A 2017 story from U.S. News [9] found that nearly every state has a law banning the use of skimmers to fraudulently obtain credit card information and that some states are increasing penalties.

While this is also an affirmative step taken by the states, it does not completely prevent financial losses. Despite efforts to educate consumers, find and remove skimmers, and increase criminal penalties, it appears that skimmers will continue to be an issue for which a solution will need to be found.

By:
Monday, February 26, 2018 at 12:24 PM
Tags: