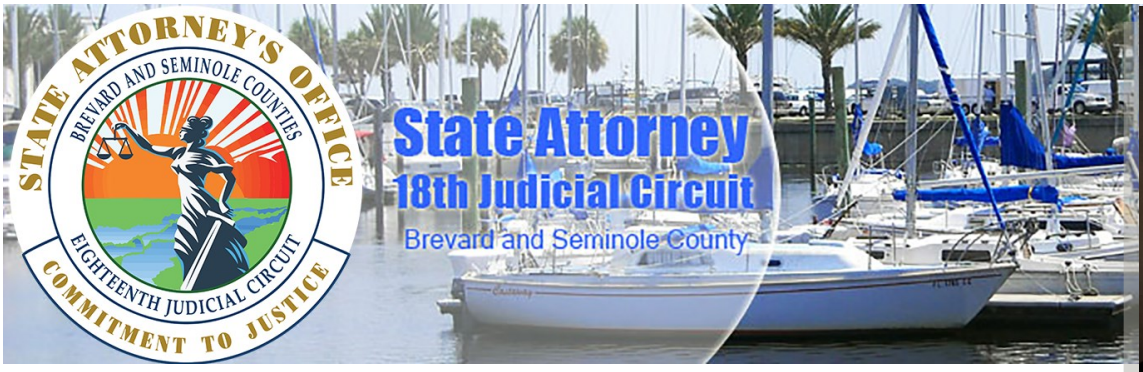

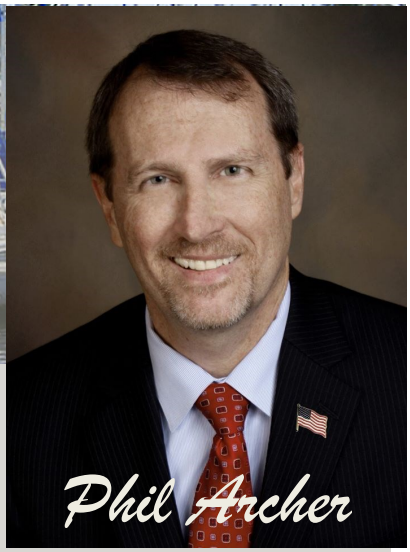

The Monthly Brief

Volume 10 Issue 7 July 2023

Gas Pump Skimmers

Credit card–skimming devices are covertly installed on gas pumps and allow thieves to take information off your credit card when you insert it. Florida law makes that activity a felony, but you have a role also.

A card skimmer works by being placed in or behind a card slot and reads the magnetic strip on your card along with the real pump reader. The charge goes through with no indication the data has been stolen. At risk gas pumps aren't continuously monitored or are not clearly visible to attendants.

Card skimmers are designed to look like part of the point-of-sale hardware. They are usually bulky and plastic, stick out further than the machine, and have arrows that don't line up. The device may also wiggle because it's not a permanently affixed piece of the machine. Card skimmers can also be placed inside the machine, transmitting stolen data remotely.

Educate yourself on how to spot a credit card skimmer. Look at other machines and compare the appearance of readers. Check the lockable door for a broken tape seal or damage.

Use the pump closest or in clear view of the attendant. Don't use a debit card, or use it only as a charge where you don't enter your PIN number. Set up alerts for your card whenever the card isn't present and is used. A chip card is safer as it can be read without being inserted. Apple Pay creates a unique code for each transaction or consider paying through a gas app on your phone. For more visit FDACS, RD.com, Capital One, and view these ABC 7 and ABC 33/40 videos.

Follow Us On Facebook

Subscribe: philarcher@sa18.org

DMV Data Breach = Credit Freeze

A recent data breach compromised the information of 3.5 million people in Oregon and 6 million in Louisiana. The Oregon Department of Transportation said at least driver's licenses were exposed in the breach, while the Louisiana Office of the Governor said in addition to driver's licenses, Social Security numbers, names, addresses and other personal information is at risk. When social security numbers and names are exposed, you may wish to consider the extra step of a Credit Freeze. It won't affect credit scores and it's more difficult for criminals to open new accounts in your name. Here's how to do that with the big 3 credit reporting agencies.

Experian: Visit the Security Freeze webpage to log-in or create an account, then fill in the details. You can also call them at 1-888-EXPERIAN (1-888-397-3742). A security freeze will remain on your credit file until you remove it.

Equifax uses a similar online process with their Equifax Security Freeze page. Log in (or create an account) and follow the steps. If you need help, you can call them at 1-866 -478-0027. You can also place a one-year fraud alert on your credit report at no cost.

TransUnion has a Credit Freeze page and click "Add A Freeze". You'll be prompted to create an account or log in. Fill in your details, and TransUnion will take care of the rest. If you have any questions, you can call them at 1-888-909-8872. To learn more about credit freezes and alerts visit the FTC's website. *SecurityBoulevard, ODOT, Equifax, TransUnion, Experian, WWLTV

Federal Trade Commission Fraud Report

The Federal Trade Commission has issued its Data Book on fraud reports for 2022. U.S. consumers reported $9 billion in fraud losses, compared to $6.1 billion the year prior. Because fraud often goes unreported, this report only shows the tip of the iceberg.

Investment Scams Up - Reported losses increased from $1.8 billion in 2021 to a total of $3.9 billion in 2022, with median losses reported at $5,000. Cryptocurrency played a big role with reported losses at $1.4 billion. 74% of adults who reported an investment scam reported a loss; this is significantly higher than other fraud type.

Impostor Scams Still on Top - Once again, impostor scams were the top category of fraud in 2022, with reported losses exceeding $2.7 billion. #1 contact method was email (76,000), but not far behind was a phone call (70,000). Impersonating businesses topped government impostor fraud reports in 2022.

More than anything, the report shows that no one is immune to fraud. Adults under age of 30 made up 43% of all fraud reports, while older adults reported losing the most money. Social media-based scams netted a reported $1.2 billion, more than any other method. However, those who reported losing money to phone scams lost more, with an average loss of $1,400.

Visit the AARP website for more info on investment fraud and imposter scams For more data and reports visit the FTC Sentinel Data Book page. * AARP, FTC