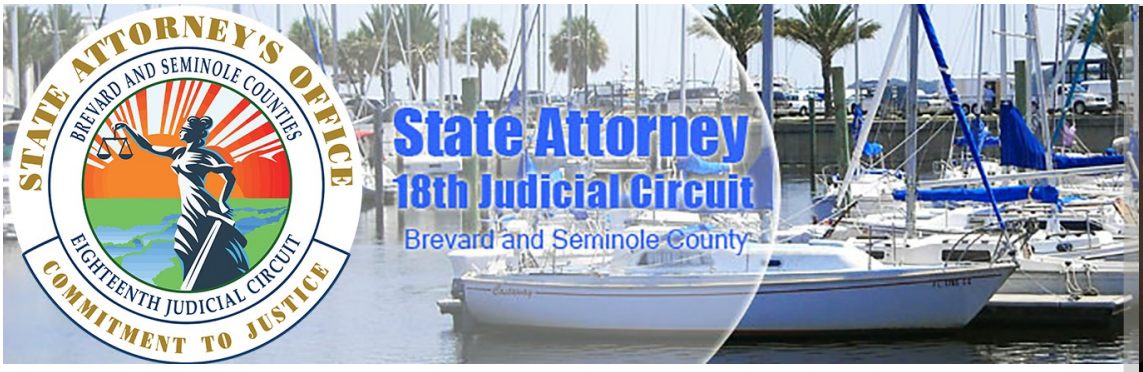

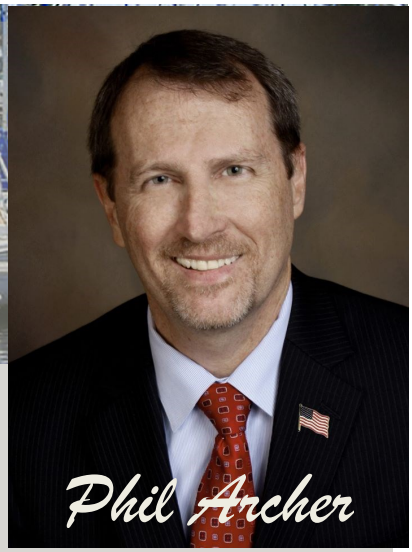

The Monthly Brief

Volume 9 Issue 8 August 2021

Scams At A Glance

Florida Attorney General Ashley Moody provides a valuable resource for consumers in their battle against fraud. The website "Scams At A Glance" provides detailed and up-to-date information, with help to avoid becoming a victim of commonly reported scams.

In addition, the site also offers free, easy to read brochures (in both English and Spanish) that can be downloaded, printed and shared with seniors and others with limited technical skills or internet access.

Topics with brochures on the site include:

IRS Impostors: Scams usually begin with a phone call from someone posing as an IRS agent claiming that a person failed to file their tax return or owes back taxes.

Tax Identity Theft: warning signs that a fraudulent tax return may have been submitted and tips to help prevent tax identity theft.

Price Gouging: During a declared state of emergency, bad actors might try to take advantage by unfairly raising the price of essential items and supplies.

Phantom Debit: Is any debt that does not exist, has already been paid or has previously been discharged.

Other scam topics include Coronavirus Scams, Moving Scams, Sweetheart Scams, Identity Theft, Holiday, Technical Support, Veteran and Natural Disaster Scams.

For more about these and other scams, or to download free brochures to print or email, visit MyFloridaLegal.com/ScamsataGlance

*FL AG Ashley Moody

Follow Us On Facebook

Subscribe: philarcher@sa18.org

Credit Card Skimmers

A problem for years, these always evolving gadgets have been ripping off consumers nationwide. The common method is to use a card reading device on the pay point at the gas pump or ATM to capture credit or debt card info. Criminals then skim or clone your card and start draining your bank account or run up charges to your credit card.

These devices fall into 2 basic types. Overlay (Skimmer) or Internal (Shimmer).

Overlays fit over the card reader slot to capture the card number and a camera mounted on or above the machine records your pin code entry. The internal device mounts inside the card slot and uses onboard microchips to read and record your card number and pin from the magnetic strip. Best defense? Chip cards with extra security can prevent skimmers from unlocking your card info. It's not perfect, but much, much more secure.

Also, look the machine over, is the security seal intact? Wiggle the reader, nothing should be loose or come off. Compare your pump to other pumps, are they the same? Use a pump in view of a clerk. Avoid debit cards, use a credit card to protect your bank accounts. Sign up for card use text alerts, as stolen cards will often be used immediately.

Learn more about these devices, including photos and videos of what to look for, along with more tips on protecting yourself by visiting Security Bank, PC Magazine, and Kim Komando.

*SNBSD, PC Magazine, Komando. com

Verizon Impersonator

Most of us have a mobile phone and we keep it close in case of emergency, or to stay in touch with anyone who might need us. It's a vital device and why this customer service imposter scam is so alarming.

A woman in Arizona recently received a phone call from someone claiming to be with Verizon, which happened to be her mobile carrier. The alleged Verizon employee told Sarah that someone was trying to break into her account, according to CBS TV3. The caller requested access to Sarah's account to stop it, and she gave her credentials to them. The caller turned out to be a scammer who used Sarah's account to purchase three iPhone12 Pro Max smartphones for a total of $3,200. She wasn't aware of it until she checked her Verizon account sometime later. According to Sarah, Verizon said that the phones were picked up at a Verizon store by somebody who was not asked to provide identification. That's a terrible business practice and ultimately Verizon agreed not to charge Sarah for the stolen phones.

Here are some tips to avoid this and other account alert imposter scams. **Go to the Source**: If you get a call, email, or text about an issue with any account, don't respond there. Go directly to the service, login and check you account. **Don't give out Credentials**: Legitimate businesses will not ask for this information over the phone **Don't panic:** If you feel pressured or rushed, it's scam. **When in doubt, hang up:** If you feel nervous or suspicious, hang up the phone and give yourself time to think. Learn more about impostor scams by visiting the AARP and USA.gov

* AARP, USAgov,CBSTV3