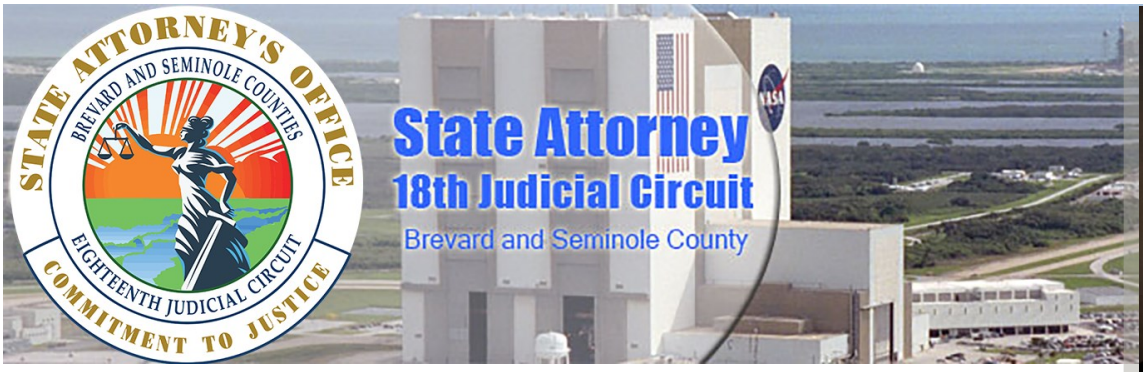

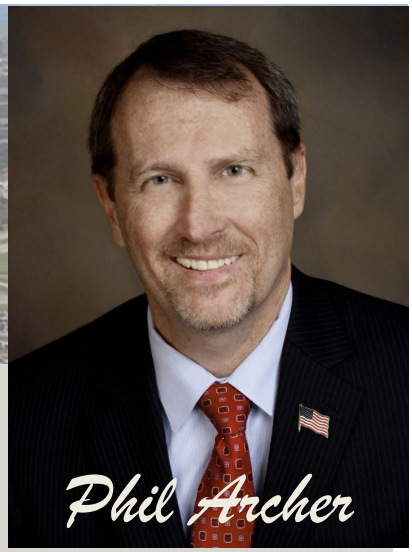

The Monthly Brief

Volume 11 Issue 8 August 2023

AG Scam Resources

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 www.myfloridalegal.com/scams-at-a-glance *FL AG Ashley Moody

Follow Us On Facebook

Subscribe: philarcher@sa18.org

AI Is Changing Fraud

One of the ways scammers remain relevant is using technology. They are always looking at new ways to steal money and information. These days that is happening in the world of artificial intelligence—commonly known as AI. Using this tech with only a few seconds of someone's voice (captured from social media videos), criminals can use AI voice-cloning to create a computer generated version that can say anything. Imagine getting a phone call from a child or grandchild saying they are in trouble and need money. Normally we'd be skeptical, but the voice you hear now sounds exactly like your loved one. It may not be long till they can create a look-a-like video also.

AI "chatbots" can clean up many of the grammar errors that are common to scam emails or texts. This removes a typical red flag that consumers have gotten good at spotting. We're also seeing online ads for AI tools you can download and use for free. This can be dangerous as crooks are using these ads to take victims to fake websites that install malware or try to obtain your personal information.

Remember that no matter how convincing, scams will always ask for money or sensitive information. Urgency created by an unexpected/unsolicited email is your warning to disengage. Always verify by calling a known good number or family member. Never trust a link in an email, text, or online ad. Type in the destination website yourself to ensure you aren't sent to a fake version of the site. Learn more by visiting Michigan AG, the FTC and Fox Business. *AARP, FTC, FoxBusiness, MIAG

Brand Name Impersonators

We all have accounts with brand name businesses like banks, mobile providers, and dozens of retailers. That's why customer service imposter scams are skyrocketing. From fake listings on the internet to emails, calls, and texts alerts about your accounts, there's a lot to watch out for. Emails and text messages containing links and dire warnings about your account security or fraudulent charges, are common. Live or recorded calls about suspicious activity on your Amazon or Bank of America account are examples. Alerts that a package can't be delivered due to problems with your address are on the rise. AARP says that letters posing as mortgage lenders warn of issues with your loan and contain a QR code for you to scan. This links to a malicious website or call center. Red flags include only generic info about your account. Asking for verification info like a credit card or social security number. Asking for payment to resolve the issue, typically by gift card, wire transfer, or for remote access to your computer by having you download and install software.

Here are some tips to avoid 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 your 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, ABC News