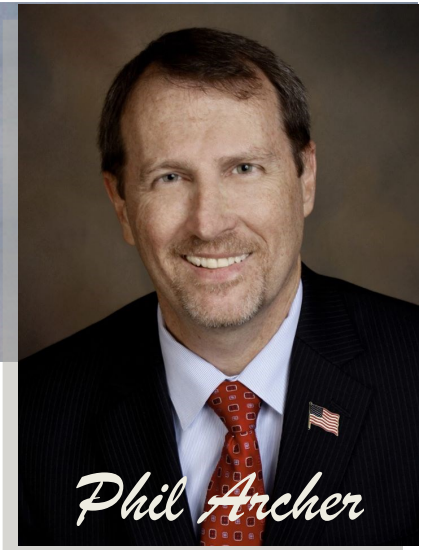




State Attorney
18th Judicial Circuit
Brevard and Seminole County



Saluting Service



Phil Archer

The Monthly Brief

Volume 10 Issue 11

November 2022

CHARITY CHECK



Scam charities and crowdfunding campaigns use natural disasters to target those looking to help others in need. To combat this trend the BBB is offering tips along with a list of [BBB Accredited Charities](#) that are engaged in disaster relief activities.

Is the disaster appeal clear? The donation request should identify what disaster relief activities you are supporting. Don't assume what they do based solely on the group's name.

Does the charity already have a presence in the impacted area? If so they are more likely to deliver help quickly.

Is the charity established & experienced? These organizations will be able to provide help with greater speed and efficiency than a newly created effort.

If crowdfunding, do you know the groups organizers? Some sites vet postings after a disaster, others don't. Review the site's policies and procedures to find out. If in doubt, it is always safest to donate to people who you personally know and trust.

The BBB has evaluated and [listed on their website several charities](#) offering assistance to victims of hurricane disaster based on 20 standards of accountability. You'll find info identifying the charity, and specific disaster relief information.

Also visit BBB's [Give.org](#) to access free evaluative reports on other charities, along with helpful tips and information to help you to ensure your giving goes where you intend it to.

*Source BBB

Follow Us On Facebook

Subscribe: philarcher@sa18.org

Package Delivery Scams

Online shopping is more popular than ever making it a prime target for scammers all year long. Now crooks are calling, emailing, and texting victims posing as a mail carrier or delivery service (USPS, FedEx, UPS) claiming they were unable to deliver a package. If you're not expecting a package the crooks try to convince you it's a gift from friend or relative. The callers sound professional and the emails and texts look legit, even containing logos and no grammatical errors. If you respond the game is on.

The caller will ask you to verify personal information or give them your credit card to reschedule the delivery. Email messages may ask you to click on a tracking link for your mystery package. When you click, you may download malware onto your computer that could give access to any personal information and passwords. No matter the method of contact, the package doesn't exist. Sharing your personal information puts you at risk for identity theft. Here are some ways to avoid Package Delivery Scams.

Beware of unsolicited communications. Delivery companies typically don't call or text and email only if the customer has signed up for alerts. **Track your packages.** Being familiar with your orders makes it hard for crooks to fool you. **Don't give out personal info.** Hang up, look up the customer service number and confirm the info yourself. **Never click on links** in unsolicited emails and texts. Go directly to the company website using your secure browser and security software. For more info visit the [BBB](#), [FedEx](#), [USPS](#), and [UPS](#) websites.

*Source BBB, FedEx, USPS, UPS

MEDICARE OPEN ENROLLMENT CONS



Medicare open enrollment runs from Oct. to Dec. allowing participants to make changes to their coverage, and others to enroll. With the popularity of the program, scammers are targeting participants for fraud. [AgingCare](#), [FTC](#), [AARP](#), and other [media outlets](#) are reporting on scams that are being used:

Phone calls from someone claiming to represent Medicare requesting your Medicare number and credit card information to sign you up for health coverage. Or asking you to confirm your Medicare number, personal info, banking details, or billing address as part of an account update. Some calls involve the false claim that signing up for Part D prescription coverage is required to maintain Medicare benefits. It's not, and totally optional coverage. [Check out this informative video from Fox 10 News in Mobile AL](#)

In another version, victims are called and told they are owed a Medicare refund. The call has potentially the biggest data payoff for a scammer, as they will often try to obtain your birth date, Social Security number, bank account and Medicare numbers.

Here are some tips to avoid these Medicare Scams:

1. Medicare will never phone you to sign up for plans or coverage.
2. Medicare will never cold call and cannot ask for payment information over the phone or online.
3. Never give out your personal info, Medicare number, banking details, or Social Security number to anyone you don't know or trust. For more info or questions visit [Medicare](#) or call 800-Medicare (633-4227). Or the [AARP Hotline](#) at 877-908-3360.

* Source AARP, Komando.com, Medicare, AgingCare, FTC, Fox 10