## **DISASTER CHARITABLE SOLICITATION FRAUD**

The Pennsylvania State Police (PSP) is reminding residents to be alert for solicitation fraud that may appear as email solicitations, phone solicitations, or pop-up charities as a result of Hurricane Florence. After a natural disaster occurs, many people rush to financially help those in need. Criminals lurk in the shadows of natural disasters and prey upon vulnerable individuals and organizations hoping that generous people, in their eagerness to assist, will donate without vetting the charity. The scammer's plan is to profit from your intended donation. When you decide to support a cause you care about, you want your donation to go to a legitimate organization. The PSP recommends doing some research and planning to help ensure your donations are used to support the intended cause. Below are tips to help you plan your donation and to avoid scams:

- Never provide personal information such as your social security number, date of birth, credit card number, or address
- Be suspicious of any stranger calling asking for money, regardless of the situation
- Government agencies will never call to ask you to verify personal information or request payment
- Educate yourself about scams and tips to avoid being a victim: <a href="Phone Scams">Phone Scams</a> | Consumer Information</a>
- Verify the legitimacy of any email and/or telephone solicitation by researching the organization or calling the company back
- Do not assume charities that are posted on social media or on the internet are legitimate. The Federal Trade
  Commission recommends vetting any charity with the Better Business Bureaus' suggested websites: give.org,
  charitynavigator.org, charitywatch.org, and guidstar.org
- When you consider giving to a specific charity, search its name plus "complaint," "review," "rating," or "scam."
- Be aware of copycat names and names similar to those of legitimate charities
- Make sure that you are on the correct website of the organization and not a copycat website. Watch for misspellings or improper English
- Most legitimate charity websites end in .org rather than .com
- Never click on attachments and links in unsolicited emails
- Designate the disaster to ensure your funds go toward disaster relief
- Legitimate charities do not normally request donations in cash, gift cards, or via money transfers
- To be safer, pay by credit card or check. Never write a check payable to individuals
- Donate to charities you know and trust. Find your state charity regulator at <u>nasconer.org</u><sup>1,2</sup>

The best way to stop scams and fraud is through vigilance. Be aware of how fraudulent schemes work and protect yourself accordingly. If you think you have been the target of a scam, make sure to report it by filing a complaint with the Federal Trade Commission at <a href="https://www.ftccomplaintassistant.gov">www.ftccomplaintassistant.gov</a> or 1-877-FTC-HELP.

<sup>&</sup>lt;sup>1</sup> FBI. (2018, September 11). Potential for Fraud and Corruption in the Aftermath of Hurricane Florence. LIR 180911001.

<sup>&</sup>lt;sup>2</sup> Federal Trade Commission. (n.d.). Before giving to a charity. *FTC*. Retrieved 09/13/2018 from <a href="https://www.consumer.ftc.gov/articles/0074-giving-charity">https://www.consumer.ftc.gov/articles/0074-giving-charity</a>.