NGB Watchdog

Tips on Avoiding Fraudulent Charitable Contribution Schemes

The National Center for Disaster Fraud reminds the public to be aware of and report any instances of alleged fraudulent activity related to relief operations and funding for victims. Unfortunately, criminals can exploit disasters, such as Hurricane Harvey, for their own gain by sending fraudulent communications through email or social media and by creating phony websites designed to solicit contributions.

Tips should be reported to the National Center for Disaster Fraud at **(866) 720-5721**. The line is staffed 24 hours a day, seven days a week. Additionally, e-mails can be sent to **disaster@leo.gov** (link sends e-mail), and information can be faxed to **(225) 334-4707**.

The U.S. Department of Justice established the National Center for Disaster Fraud to investigate, prosecute, and deter fraud in the wake of Hurricane Katrina, when billions of dollars in federal disaster relief poured into the Gulf Coast region. Its mission has expanded to include suspected fraud from any natural or manmade disaster. More than 30 federal, state, and local agencies participate in the National Center for Disaster Fraud, which allows the center to act as a centralized clearinghouse of information related to disaster relief fraud.

The public should remember to perform due diligence before giving contributions to anyone soliciting donations or individuals offering to provide assistance to those affected by the hurricane and tornadoes. Solicitations can originate from social media, e-mails, websites, door-to-door collections, flyers, mailings, telephone calls, and other similar methods.

Before making a donation of any kind, consumers should adhere to certain guidelines, including:

- Do not respond to any unsolicited (spam) incoming e-mails, including clicking links contained within those messages, because they may contain computer viruses.
- Be skeptical of individuals representing themselves as members of charitable organizations or officials asking for donations via e-mail or social networking sites.
- Beware of organizations with copy-cat names similar to but not exactly the same as those of reputable charities.
- Rather than follow a purported link to a website, verify the legitimacy of nonprofit organizations by utilizing various Internet-based resources that may assist in confirming the group's existence and its nonprofit status.
- Be cautious of e-mails that claim to show pictures of the disaster areas in attached files because the files may contain viruses. Only open attachments from known senders.
- To ensure contributions are received and used for intended purposes, make contributions directly to known organizations rather than relying on others to make the donation on your behalf.
- Do not be pressured into making contributions; reputable charities do not use such tactics.
- Be aware of whom you are dealing with when providing your personal and financial information. Providing such information may compromise your identity and make you vulnerable to identity theft.
- Avoid cash donations if possible. Pay by credit card or write a check directly to the charity. Do not make checks payable to individuals.
- Legitimate charities do not normally solicit donations via money transfer services. Most legitimate charities' websites end in .org rather than .com.