Tips for Identifying or Avoiding Becoming a Victim of Disaster Fraud

Below are some tips provided by the FBI to help identify potential disaster fraud, and to help avoid becoming a victim of fraudulent charitable solicitations.

If you know about or suspect fraud, waste, abuse or allegations of mismanagement involving disaster relief operations, you can report it through the **National Disaster Fraud Hotline, toll free, at (866) 720-5721 or the Disaster Fraud e-mail at disaster@leo.gov**. The telephone line is staffed by a live operator 24 hours a day, seven days a week.

Identifying Disaster Fraud

The following questions are designed to assist in identifying potential fraud:

- Are you aware of any individuals or groups fraudulently receiving disaster assistance that they are ineligible to receive, for instance: someone living outside of the impact area at the time of the disaster; the property did not exist or property was not owned by the claimant; someone has applied multiple times using fictitious information or committing identity theft; the person was incarcerated at the time of the disaster?
- Are you aware of any scheme that enables any individuals (including public officials) or businesses to take advantage of program details or procedures in order to defraud the government?
- Are you aware of any entities committing disaster fraud by inflating invoices, billing for overtime not earned, or otherwise receiving federal disaster funding fraudulently?
- Are you aware of any schemes that take advantage of emergency rule changes to defraud the government, for example, emergency procurement rules that raise or limit competition requirement limits?

Making Charitable Donations

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.