Excerpts taken from CUNA Mutual Group Risk Alert, April 5, 2022

Ukrainian relief efforts are being launched across the nation. Unfortunately, as with most national or global tragedies, the scam artists quickly arrive and prey on the empathy of individuals, including credit union members, with fundraising schemes. If you are making donations, it is always encouraged to conduct proper due diligence to ensure funds are going to legitimate organizations and recipients.

Details

In unpredictable situations, such as the crisis in Ukraine, a brighter financial future can seem almost impossible. Leading with empathy and helping people get access to their basic human necessities, such as medical care and food, is one of the ways to show up to support those in our communities during difficult times.

However, some individuals with sincere intentions to donate to just causes – such as Ukrainian relief efforts - are falling victim to fraudsters ceasing the opportunity to tug at their heartstrings. It is common for scammers to seek people, including credit union members, out so it can be easy to fall victim to a scam.

Scam artists use contact methods including phone calls, texts, and emails (often with a link to a spoofed website, or an attachment), social media networks, banner ads, and the internet. The scammers typically pose as friends, family, or romantic interests on social media to request donations.

Reasons given often mirror valid reasons for a legitimate charitable organization such as:

- The need to relocate a family or child within or outside the country
- Their home has been destroyed
- The need for medical or rebuilding supplies including medication and food

Key red flags include a sense of urgency and requesting donations in the format of gift cards, wire transfers or cryptocurrency.

How to safely donate and protect yourself this and other types of fraud:

- Do not click on a link or attachment to donate online in an email received from someone unknown to you.
- Connect through a different communication link to verify the request if an unsolicited online donation request is received from a friend or family member.
- Do not provide Personal Identifying Information (PII) or debit /credit card numbers in response to an unsolicited charitable request.
- Resist high pressure tactics and those with a sense of urgency. Be aware of direct emails from “victims” and solicitors who have a heart wrenching story.

- Research the organization requesting the donation and if you do not feel comfortable, proactively research charitable organizations you may be more familiar with if you would like to donate. Look up the relief effort through a site such as BBB Wise Giving Alliance, Charity Navigator or CharityWatch.
- Read online reviews. Then, enter the URL of the charity yourself to independently confirm you are coordinating with the right organization.
- Be wary of proactive outreaches requesting wire transfers and cryptocurrency and do not donate gift cards.
- If donating to a charity's website, make sure the website is secure, your internet connection is secure, and your computer is equipped with the latest anti virus protection.
- If possible, always pay by credit card, which offers additional layers of protection.
- If donating via check, always make the check payable to the charity instead of an individual.

If you think you are the victim of a scam, contact NHFCU immediately at (603) 224-7731.