Bond
INFORMATION MEMO
NOVEMBER 10, 2020

# IRS Dirty Dozen Includes Tax Scam Targeting Charitable Giving

In most years, the IRS's annual "Dirty Dozen" list of trending tax scams is not required reading for nonprofits. However, as with everything else, this year has proven to be an exception to the rule[1]: the 2020 Dirty Dozen includes an alert to the public that scammers, who often take advantage of natural disasters and other crises to solicit fraudulent donations, have been doing so under cover of the global COVID-19 pandemic. Most concerning for the nonprofit sector, scammers are not only soliciting donations for fake charities, but are also diverting donations intended for real charities.

### Fake Solicitations for Fake Nonprofits

According to the IRS, scammers are now increasing efforts to exploit the impact of COVID-19 by setting up fake charities to solicit donations from well-intentioned individuals who are trying to assist their communities. This of course reduces funds that would otherwise be deployed by legitimate nonprofit organizations to support their communities and carry out their missions, as intended by the would-be donors.

### Fake Solicitations for Real Nonprofits

Even more disturbing, fraudulent solicitations are increasingly taking the form of "phishing." Phishing is usually accomplished through the use of unsolicited digital communications – emails, letters, texts and website links – designed to trick potential victims into engaging with the scammer (by clicking on a link or responding to a text or email), who is acting in the guise of a legitimate nonprofit. As described by the IRS:

> *Fraudulent schemes normally start with unsolicited contact by telephone, text, social media, e-mail or in-person using a variety of tactics. Bogus websites use names similar to legitimate charities to trick people to send money or provide personal financial information. . . .*
>
> *Taxpayers should be particularly wary of charities with names like nationally known organizations. Legitimate charities will provide their Employer Identification Number (EIN), if requested, which can be used to verify their legitimacy.*

### What can your organization do?

Nonprofits should be vigilant of illegitimate websites and phishing schemes that could target their donors and communities. Use of your organization's name should be monitored on social media and in other internet contexts. You may want to proactively advise your donors of the emergence of this danger and enlist their help.

If you or your organization have any questions or concerns related to the threat of tax scams during COVID-19 and beyond, please contact Thomas W. Simcoe, Delaney M. R. Knapp or the attorney at the firm with whom you are regularly in contact.

---

1 Internal Revenue Service, IRS Unveils "Dirty Dozen" List of Tax Scams for 2020; Americans Urged to be Vigilant to These Threats During the Pandemic and Its Aftermath (July 16, 2020), available here.

BOND SCHOENECK & KING ATTORNEYS