We have received reports that individuals are receiving phone calls and emails asking them to "verify their information" in order to receive a refund or a potential stimulus check. These are scams and should be disregarded.

We want to remind our clients that the **Internal Revenue Service (IRS) and other governmental agencies do not initiate contact with taxpayers by email, phone calls, text messages, or social media channels** to request personal or financial information.

HOW TAXPAYERS ARE CONTACTED

The IRS and other governmental agencies initiate most contacts with taxpayers through regular mail delivered by the United States Postal Service (USPS).

HOW TO SPOT SCAMMERS

SCAMMERS TYPICALLY:

- Use fake names and IRS badge numbers to identify themselves via bogus phone calls or emails, including using bogus caller ID tags to make a phone number appear as if the IRS or another governmental agency is calling.
- Follow up bogus phone calls with bogus emails to make the phone call appear legitimate.
- Send email links for taxpayers to "verify" information by typing that information into a bogus form.
- Ask for or ask to "verify" credit card, debit card, or bank account information over the phone.
- Ask to "verify" information such as Social Security numbers, birthdates, address, telephone number, or other personally identifiable information. **Scammers may know the last four digits of the taxpayer's Social Security number**, making the inquiry appear legitimate. The IRS or other authorities should already have your personally identifiable information on file.
- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card, or wire transfer. Generally, the IRS will first mail a notice for payment via USPS to any taxpayer who owes taxes.

WHAT YOU CAN DO

- **Do not click on links or attachments in unsolicited emails.** Scammers can **appear** to be from a legitimate organization you do business with or a person you know. They are inviting you to click on a link to a bogus website or to open an attachment on your device. The websites and attachments are often malicious and can infect your devices with malware.

- **Report IRS phone scams** to the Treasury Inspector General for Tax Administration on the **IRS Impersonation Scam Reporting** web page. You can also call 800-366-4484.

- **Report other phone scams** to the Federal Trade Commission. Use the **FTC Complaint Assistant** on FTC.gov. Please add "IRS Telephone Scam" in the notes.

- **Report an unsolicited email** claiming to be from the IRS, or an IRS-related component like the Electronic Federal Tax Payment System, to the IRS by emailing **phishing@irs.gov**.

Do not provide personal information if you are contacted with unsolicited invitations to "verify your information" to receive a tax refund or potential stimulus check.