Treasury Inspector General for Tax Administration

Press Release

March 5, 2021 TIGTA-2021-1 Contact: David Barnes (202) 622-3062

David.barnes@tigta.treas.gov

TIGTA Urges U.S. Taxpayers to Be On the Lookout for Fraudulent Activity Concerning Pandemic-Related Scams

WASHINGTON – In support of <u>National Consumer Protection Week</u> and <u>National Slam the Scam Day</u>, J. Russell George, the Treasury Inspector General for Tax Administration (TIGTA), today urged taxpayers to beware of scams related to Economic Impact Payments (EIP) being distributed to taxpayers.

The Internal Revenue Service (IRS) has issued billions of dollars of EIPs to taxpayers by direct deposit, as well as by U.S. Treasury check or debit card via U.S. Mail.

TIGTA's Office of Investigations warns that criminals may engage in various scams and schemes in attempts to intercept EIPs. Criminals may also try to steal sensitive taxpayer information as the pandemic enters its second year.

TIGTA oversees Federal tax administration and investigates fraudulent activity related to the distribution of funds by the IRS, such as EIPs.

"In these troubled times, crooks and scammers will try to defraud taxpayers in every way possible," Inspector General George stated. "Taxpayers need to be especially vigilant when contacted by individuals claiming to be from the IRS."

Taxpayers may encounter fraudulent IRS websites, or receive social media-based communications and/or phishing e-mails, text messages, or other communications that claim to be from the IRS, that ask for sensitive personally identifiable information or payments in order to receive an EIP. These are scams. Taxpayers should not click on any embedded links, scan any quick response – commonly referred to as "QR" - codes, or open any attached files. Scammers may use these methods to install malicious software on a victim's phone or computer.

Scammers may also try to convince victims to deposit fraudulent or stolen U.S. Treasury checks into a victim's bank account. After the victim makes the deposit, the scammers request that the victim send funds from that deposit to another account, or use those funds to purchase prepaid cards. Report this type of activity to TIGTA immediately at tips.TIGTA.gov.

In order to avoid falling victim to criminals impersonating IRS employees or otherwise falsely claiming to represent the IRS, TIGTA offers the following tips:

• The IRS will not call you, text you, or e-mail you to request information as a prerequisite to receiving an EIP.

- To check on the status of your EIP, visit www.IRS.gov and click on "Get Coronavirus Tax Relief" and then select "Get My Payment." Only use the website www.IRS.gov. Do not use any other websites or services that claim to be able to process your EIP or act as an intermediary between you and the IRS. Similarly, do not click on any links in e-mails that purport to take you to the IRS website. The best practice is to manually type "www.IRS.gov" into your web browser.
- Anyone who calls you claiming to be from the IRS and offering to process your EIP is impersonating the IRS. Do not share any personal or financial information with these scammers. Hang up the phone and report this activity on our website at tips.TIGTA.gov.
- Do not share your personal information with anyone claiming to be from the IRS offering to assist you with your EIP.
- Do not share your online banking username or password with anyone. The IRS does not need your online banking username and password in order to send your EIP.

After your EIP is processed, the IRS will send you a letter confirming your payment. If you receive this letter, but you have not received your EIP, please report the missing payment to TIGTA through our website at tips.TIGTA.gov. You will also need to report the missing payment separately to the IRS.

###