Many scammers are targeting customers. You should always remain on the alert for potential suspicious activities. Financial red flag indicators of imposter scams may include:

1. A customer indicating that a person claiming to represent a government agency contacted him or her by phone, email, text message, or social media asking for personal or bank account information to verify, process, or expedite EIPs, unemployment insurance, or other benefits.[12] In particular, be alert to communications emphasizing "stimulus check" or "stimulus payment" in solicitations to the public, sometimes claiming that the fraudulent entity can expedite the "stimulus check" or other government payment on behalf of the beneficiary for a fee paid by gift card or prepaid card.

2. Receipt of a document that appears to be a check or a prepaid debit card from the U.S. Treasury, often in an amount less than the expected EIP, with instructions to contact the fraudulent government agency, via a phone number or online, to verify personal information in order to receive the entire benefit.

3. Unsolicited communications from purported trusted sources or government programs related to COVID-19, instructing readers to open embedded links or files or to provide personal or financial information, including account credentials (e.g., usernames and passwords).

4. Email addresses in COVID-19 correspondence that do not match the name of the sender, contain misspellings, or do not end in the corresponding domain of the organization from which the message allegedly was sent. For example, government agencies will use ".gov" or ".mil." Many legitimate charities will use ".org." WHO emails will contain "@who.int." Fraudsters, however, may use ".com" or ".biz" in place of the expected domain.

5. Email correspondence that contains subject lines that government or industry have identified as being associated with phishing campaigns, or that contains embedded links or webpage addresses for purported COVID-19 resources that have irregular URLs (e.g., slight variations in domain extensions like ".com," ".org," and ".us"). Examples of U.S. government-identified COVID-19 phishing email subject lines include "2020 Coronavirus Updates," "Coronavirus Updates," "2019-nCov: New confirmed cases in your City," and "2019-nCov: Coronavirus outbreak in your city (Emergency)."[13]

6. Solicitations where the person, email, or social media advertisement seeks donations on behalf of a reputable organization, but is not affiliated with the reputable organization (e.g., the solicitor is not recognized or endorsed as an employee or volunteer by the organization, the email address is misspelled or not connected to the organization, or the social media advertisement directs individuals to an unaffiliated website).

7. A charitable organization soliciting donations that (1) does not have an in-depth history, financial reports, IRS annual returns, documentation of their tax-exempt status, or (2) cannot be verified by using various internet-based resources that may assist in confirming the group's existence and its nonprofit status.

11. *See* FTC, "How to Donate Wisely and Avoid Charity Scams."

12. For more information on EIPs, visit IRS, "Economic Impact Payment Information Center," (June 30, 2020).

13. *See* DHS CISA and U.K. NCSC Alert, "COVID-19 Exploited by Malicious Cyber Actors," (April 8, 2020).