

FRAUD & SCAM AWARENESS



PANDEMIC IMPOSTOR SCAMS: RED FLAGS

Recently, the Financial Crimes Enforcement Network (FinCEN) released an advisory about pandemic related impostor scams and money mule schemes. **Here are three red flag situations you should be aware of:**

- 1. You are contacted by an alleged government representative** to verify, process, or to expedite an economic impact payment.
- 2. You receive a receipt that seems to be a check** or prepaid debit card from the US Treasury, but it has suspicious characteristics. For

instance, the stimulus check may be smaller than expected, or you may be given an email or phone number to contact. You are then asked to confirm your personal information, purportedly to get the rest of the benefit.

- 3. You receive an official-looking correspondence** from email addresses that don't match the name of the sender or use ".com" or ".biz" instead of ".gov" or ".mil," which are official government domains.

If you suspect a situation to be fraudulent, always verify with a trusted source, like your financial institution.

WHAT'S A MONEY MULE?

Scammers may try to use you to move stolen money. If you help them, you could be what law enforcement calls a money mule.

Money mule scams happen in several ways. The story often involves scams related to online dating, work-at-home jobs, or prizes. Scammers send money to you, sometimes by check, then ask you to send (some of) it to someone else. They often want you to use gift cards or wire transfers. Of course, they don't tell you the money is stolen, and they're lying about the reason to send it. And there never was a relationship, job, or prize — only a scam.

What happens next? If you deposit the scammer's check, it may clear but

then later turn out to be a fake check. The bank will want you to repay it. If you give the scammer your account information, they may misuse it. You could even get into legal trouble for helping a scammer move stolen money.

How can you avoid money mule scams?

Don't accept a job that asks you to transfer money. They may tell you to send money to a "client" or "supplier." Say no. You may be helping a scammer move stolen money.

Never send money to collect a prize. That's always a scam, and they might be trying to get you to move stolen money.

Don't send money back to an online love interest who's sent you money. Also always a scam — and another a way to get you to move stolen money.

Criminals are good at making up reasons to help them move money. Please don't do it. The funds may be from other people they scammed. You may be assisting criminals to hurt people just like you.

If you think you might be involved in a money mule or money transfer scam, stop transferring money. Notify First Western Bank & Trust or any gift card companies involved. Then, report it to the FTC at [ftc.gov/complaint](https://www.ftc.gov/complaint).

