

# FinCEN Guidance On Pandemic Fraud Scams

There are objects that people used to think protected them from poisons, including opals, emeralds, and sharks' teeth. Wouldn't it be nice if it were that easy to protect against fraud?

It's an unfortunate reality that fraudsters remain relentless in times of crisis. It's imperative for our customers to be on alert for possible warning signs because, oftentimes, you will be targeted directly.

Here are some pandemic-related impostor scam **red flags** to watch out for.

- **Contact by an alleged government representative** for the purpose of verifying, processing, or expediting a customer's economic impact payment.
- **Receipt of what seems to be a check** or prepaid debit card from the US Treasury, but has suspicious characteristics. For instance, the stimulus check may be smaller than expected or recipients may be given an email or phone number to contact where they are then asked to confirm their personal information, purportedly to get the rest of the benefit.
- **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.