FEDERAL TRADE COMMISSION

Consumer Information

Help COVID-19 contact tracers, not scammers

June 25, 2020

by Shameka L. Walker
Attorney, Division of Consumer & Business Education, FTC

Contact tracing call?

5 things to know

A contact tracer from your state health department might call if you've been exposed to COVID-19. But scammers are pretending to be contact tracers, too. Here's how you can spot the scam.

Real contact tracers won't ask you for money.

Only scammers insist on payment by gift card, money transfer, or cryptocurrency.

Contact tracing doesn't require your bank account or credit card number.

Never share account information with anybody who contacts you asking for it.

Legitimate contact tracers will never ask for your Social Security number.

Never give any part of your Social Security number to anyone who contacts you.

Your immigration status doesn't matter for contact tracing, so real tracers won't ask.

If they do, you can bet it's a scam.

Do not click on a link in a text or email.

Doing so can download malware onto your device.

Talking to a real contact tracer helps stop the spread of COVID-19. Reporting scammers helps stop them, too. Report fake contact tracers to your state and at **ftc.gov/complaint**.

FEDERAL TRADE COMMISSION

For more information about contact tracing **visit your state health department's website** and

ftc.gov/coronavirus/scams

After nearly three months of stay-at-home orders, America is starting to open up again. Contact tracers, the folks who work for state health departments to try to track anyone who may have been exposed to COVID-19, are an important part of our road to recovery. But some scammers are pretending to be contact tracers so they can profit off of the current confusion. They're trying to steal your identity, your money – or both. Luckily, there are ways to tell the difference between a real contact tracer and a scammer.

A contact tracer might get in touch to discuss results of a test you know you took, or because someone you've been in contact with tested positive. Depending on how your state has set up its program (https://health.ri.gov/), legitimate contact tracers may call, email, text, or visit your home to collect information. They may ask you for:

- your name and address
- health information
- the names of places and people you have visited

Scammers will ask you to do more. Here are some things to do to protect yourself from fake contact tracers.

- **Don't pay a contact tracer.** Anyone who says you need to pay is a scammer, plain and simple.
- **Don't give your Social Security number or financial information.** There's no reason for a legit contact tracer to need your Social Security number, bank account, or credit card number.
- **Don't share your immigration status.** Legit contact tracers don't need — and won't ask for — this information.
- **Don't click on links or download anything sent from a contact tracer**. Real tracers will only send you texts or emails that say they'll be calling you — not ask you to click or download anything.

What should you do if you think you're dealing with a fake contact tracer? Check with your state health department to see if they have a way to make sure the

person contacting you is a real contact tracer. Otherwise, hang up, close the door, or don’t respond to, click on, or download anything that may be in an email or text. Then, report it to your state and tell the FTC about it at FTC.gov/complaint