



Bureau of Consumer Protection
Division of Marketing Practices

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Lois C. Greisman
Associate Director
(202) 326-3404
lgreisman@ftc.gov

October 20, 2026

Sent Via Email

Amazon, Inc.
trustandsafety@support.aws.com
abuse@amazonaws.com

*Re: Impersonation of the Federal Trade Commission by a Domain Hosted by
Amazon.com, Inc.*

Dear Amazon.com, Inc. and Amazon Web Services, Inc. (collectively, "Amazon.com"):

I write to inform you that www.reportfraudftcgov.netlify.app, a website hosted by Amazon.com, appears to impersonate the Federal Trade Commission's ("FTC") name, logo, website design, and written and video content without authorization.

As shown in the attached screenshots, reportfraudftcgov.netlify.app mirrors the official Federal Trade Commission's webpage for reporting fraud, reportfraud.ftc.gov. The upper lefthand corner of the apparent imposter webpage prominently displays the name "Federal Trade Commission," text with the FTC's genuine reporting webpage, and a replica of the FTC's seal, as well as a banner reading "An official website of the United States Government." Reportfraudftcgov.netlify.app also copies the color scheme, graphics and layout of the official FTC website and duplicates written content, including the warning: "Scammers are impersonating the FTC." Like the FTC's own webpage for reporting fraud, reportfraudftcgov.netlify.app has a link at the upper right hand corner directing consumers to "Report Now." Consumers who navigate to the imposter webform are prompted to input sensitive information such as their name, home address, email address, phone number, age, and military affiliation, which has likely effect of deceiving consumers into mistakenly providing their sensitive data to an entity they believe is the FTC.

The FTC is not affiliated with the entities or individuals operating reportfraudftcgov.netlify.app. Please be advised that it is a violation of the Rule on Impersonation of Government and Businesses ("Impersonator Rule"), 16 C.F.R. § 461, to "materially and falsely pose as, directly or by implication, a government entity or officer."

We hope to hear from you promptly regarding this important consumer protection matter. In that communication, we would appreciate it if you would please provide data or other information identifying any other webpage associated with reportfraudftcgov.netlify.app.

Page 2

Please respond directly, and direct any questions, to Sara Tonnesen, stonnesen@ftc.gov or 202-326-2879.

Sincerely,

/s/ Lois C. Greisman

Lois C. Greisman

Attachments



Report to help fight fraud!

Report Now →

Protect your community by reporting fraud, scams, and bad business practices.

Source URL: <https://reportfraudftcgov.netlify.app/>

Collection Timestamp: Wed Sep 02 2026 12:01:43 GMT+0000 (UTC)



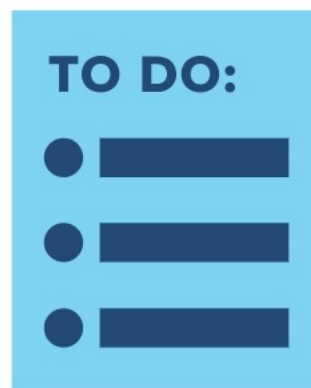
Protect your community by reporting fraud, scams, and bad business practices.

How it works



Tell us what happened

Report a scam, a company, or an unwanted call.



Get your next steps

Find out what you can do to protect yourself.



Help stop fraud

We use and share reports with our law enforcement partners to help with investigations.

Source URL: <https://reportfraudftcgov.netlify.app/>

Collection Timestamp: Wed Sep 02 2026 12:01:43 GMT+0000 (UTC)

Report a scam, a company, or an unwanted call.

Find out what you can do to protect yourself.

We use and share reports with our law enforcement partners to help with investigations.

[Get started now](#). Or you can [browse our FAQs](#).



Scammers are impersonating the FTC. Know that the FTC will never threaten you, say you must transfer your money to “protect it,” or tell you to withdraw cash or buy gold and give it to someone.

Learn more at ftc.gov/impersonators

The power of ReportFraud.ftc.gov

[Your report is shared](#) with more than 2,800 law enforcers.

Source URL: <https://reportfraudftcgov.netlify.app/>

Collection Timestamp: Wed Sep 02 2026 12:01:43 GMT+0000 (UTC)

The power of ReportFraud.ftc.gov

Your report is shared with more than 2,800 law enforcers.

We can't resolve your individual report, but we use reports to investigate and bring cases against fraud, scams, and bad business practices.

Read our [Privacy Act statement](#) to learn more about how we collect and use your information.



Source URL: <https://reportfraudftcgov.netlify.app/>

Collection Timestamp: Wed Sep 02 2026 12:01:43 GMT+0000 (UTC)



[Start your report now](#), or check out what is going on in your state or metro area by visiting ftc.gov/exploredata.

ReportFraud.ftc.gov is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

[Privacy Policy](#)



FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

[FAQs](#)

[Languages](#)

አማርኛ العربية 简体中文 繁體中文 Français Hmoob 한국어 Русский
Soomaali Español Tagalog українська Tiếng Việt Other Languages

[Report Now](#)

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.

Source URL: <https://reportfraudftcgov.netlify.app/>

Collection Timestamp: Wed Sep 02 2026 12:01:43 GMT+0000 (UTC)



FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

Search FAQs on ReportFraud.ftc.gov



FAQs

Español

Report Now →

View FAQs by topic

All FAQs

- About my report
- Filing a report
- After I file a report
- Getting my money back
- Scams
- What you can do

Frequently Asked Questions

What can we answer for you? Or view one of our FAQ topics to learn more.

Search FAQs on ReportFraud.ftc.gov



About my report

What can I report?

Report anything you think may be a fraud, scam, or bad business practice. You can report even if you didn't lose money. For ideas of what you might report to the FTC, or to get information and advice, check out [consumer.ftc.gov](#). Or go to [ftc.gov](#) to take a look at the FTC's latest cases. [Start your report now.](#)

Source URL: <https://reportfraudftcgov.netlify.app/faq>

Collection Timestamp: Wed Sep 02 2026 12:20:30 GMT+0000 (UTC)

Scams

What you can do

About my report

What can I report?

Report anything you think may be a fraud, scam, or bad business practice. You can report even if you didn't lose money. For ideas of what you might report to the FTC, or to get information and advice, check out consumer.ftc.gov. Or go to ftc.gov to take a look at the FTC's latest cases. [Start your report now.](#)

To report identity theft, go to IdentityTheft.gov.

I'm not sure if it's a scam or fraud — should I still report it?

Yes, please report it. Whether you think it's a scam, you know it is, or you're not happy about a business practice, tell the FTC. The FTC and its law enforcement partners enforce a variety of laws. Your report makes a difference and can help law enforcers spot problems. [Start your report now.](#)

Learn more about scams and how the FTC works to help stop them at consumer.ftc.gov.

I'm not sure which category to choose — what should I do?

ReportFraud.ftc.gov lists common things people report, but there are many other issues you can report to the FTC. If you're not sure which category to choose or don't see a category that fits your situation, just choose "Something Else" and describe what happened. We'll categorize it for you.

If you think your report fits in more than one category, just choose the one that fits best.

[Start your report now.](#)

Can I just report the number of an unwanted call?

Yes. When you file your report, choose the category "Just An Annoying Call." Use the streamlined form to

[Start your report now.](#)

Can I just report the number of an unwanted call?

Yes. When you file your report, choose the category "Just An Annoying Call." Use the streamlined form to report the unwanted call (like an illegal robocall). [Start your report now.](#)

For ideas on what you can do about unwanted calls, go to ftc.gov/calls.

Can I report spam texts here?

Yes. Look for the category your spam text would fit into. If you don't find one, choose "Something Else." Paste the message into the Comments field of your report — but be sure not to click on any links in the text. The FTC can't accept forwarded messages. [Start your report now.](#)

You can also report spam texts to your wireless provider and messaging app:

- Copy the message and [forward it](#) to 7726 (SPAM). This helps your wireless provider spot and block similar messages in the future.
- Report it on the messaging app you use. Look for the option to report junk or spam.
 - [How to report spam or junk in the Messages app](#)
 - [How to report spam on an Android phone](#)

Learn more at ftc.gov/TextScams.

Can I report spam and phishing emails here?

Yes. Look for the category your spam email would fit into. If you don't find one, choose "Something Else." Paste the message into the Comments field of your report — but be sure not to click on any links in the email. The FTC can't accept forwarded emails.

Can I report spam and phishing emails here?

Yes. Look for the category your spam email would fit into. If you don't find one, choose "Something Else." Paste the message into the Comments field of your report — but be sure not to click on any links in the email. The FTC can't accept forwarded emails.

[Start your report now.](#)

You can also forward unwanted messages to your email provider (like Gmail or Yahoo). Most email services include options to mark emails as spam or junk. You can also forward phishing emails to the Anti-Phishing Working Group at reportphishing@apwg.org.

Learn more about [how to get less spam in your email](#) and [how to recognize and avoid phishing scams](#).

Where should I report identity theft?

You can report identity theft and get information to help you recover at IdentityTheft.gov.

My personal information was exposed in a data breach, found on the dark web, lost, or stolen. Should I report it here?

If someone has used your information to open a new account or make a purchase, report it at IdentityTheft.gov and find out what to do next to recover.

If someone hasn't misused your information yet, you don't need to file an FTC Identity Theft Report. But there are steps you can take to help protect yourself from identity theft, including checking, freezing, and monitoring your credit. Go to IdentityTheft.gov/databreach to learn what to do.

If you don't need an FTC Identity Theft Report but want to share information about a fraud, scam, or bad business practice related to your situation, report it [here](#).

If you don't need an FTC Identity Theft Report but want to share information about a fraud, scam, or bad business practice related to your situation, report it [here](#).

I provided my personal information to someone I now think was a scammer. Should I report it here?

Yes. You can report a scam [here](#).

If you are worried about the identity theft, there are steps you can take to help protect yourself from identity theft, including checking, freezing, and monitoring your credit. Go to IdentityTheft.gov/Info-Lost-or-Stolen to learn what to do.

If someone has used your information to open a new account or make a purchase, report it at IdentityTheft.gov and find out what to do next to recover.

Can the FTC tell me if someone misused my information or freeze my credit?

No. But you can find out how to check your credit report and freeze your credit at IdentityTheft.gov/Info-Lost-or-Stolen.

What should I do if someone used my Social Security number?

Go to IdentityTheft.gov to report the misuse of your Social Security number and get a recovery plan.

If I already filed a report at IdentityTheft.gov, should I also file a report here?

You don't need to report identity theft again at ReportFraud.ftc.gov. But if you have more information about a fraud, scam, or bad business practice that exposed your information, you can report it here.

If I already filed a report at IdentityTheft.gov, should I also file a report here?

You don't need to report identity theft again at ReportFraud.ftc.gov. But if you have more information about a fraud, scam, or bad business practice that exposed your information, you can report it here.

Should I still report something to the FTC if I already reported it to another agency?

Yes, it's a good idea to report it to ReportFraud.ftc.gov, too. One exception — if you reported a financial issue to the CFPB (like debt collection, credit report, or bank issues), you don't need to report it again here.

Can I report the company I work for?

Yes. If you prefer, you can file a report anonymously. How much information you give is up to you, but filling in your contact information can help if the FTC needs more information from you. We will not automatically share your information with the company, but there are times when we may [share it](#). [Start your report now](#).

Can I file a report if I don't live in the U.S.?

If you live outside the U.S. or want to report an international scam, you can use econsumer.gov to file your report. It will then be included in the [FTC's Consumer Sentinel database](#). [Econsumer.gov](https://econsumer.gov) is a partnership of more than 65 consumer protection agencies around the world and helps identify trends and prevent international scams. It's available in English, Spanish, French, German, Korean, Japanese, Polish, Portuguese, and Turkish.

Can I file a report for someone else?

Yes. You'll be able to say if you're reporting on behalf of someone else. You'll also be able to give us your information and the information of the person you're reporting for, if you choose to share it. [Start your](#)

Can I file a report for someone else?

Yes. You'll be able to say if you're reporting on behalf of someone else. You'll also be able to give us your information and the information of the person you're reporting for, if you choose to share it. [Start your report now.](#)

Filing a report

What do I need to file a report?

Anything you can tell us about your experience is helpful. Please share as much or as little information as you'd like. If you paid any money, we'll ask how much, and when you paid. We'll also ask for any information you might have about whoever you're reporting — like their name and any contact information you have.

Can I attach or send you documents related to my report?

We can't take uploaded messages, but if you can, paste the text of your documents into the Comments field of your report. Then hold onto your documents because law enforcement might ask you for them in connection with an investigation.

Why was I sent to the CFPB to file my report?

The [Consumer Financial Protection Bureau \(CFPB\)](#) handles issues related to debt collection, credit card companies, credit reporting, and banking and might be able to help you resolve your issue. If your report falls into one of these categories, we'll send you to the CFPB's website. But don't worry — your report will still end up in the FTC's database, which makes reports available to federal, state, and local law enforcement across the country.

Source URL: <https://reportfraudftcgov.netlify.app/faq>

Collection Timestamp: Wed Sep 02 2026 12:20:30 GMT+0000 (UTC)

companies, credit reporting, and banking and might be able to help you resolve your issue. If your report falls into one of these categories, we'll send you to the CFPB's website. But don't worry — your report will still end up in the FTC's database, which makes reports available to federal, state, and local law enforcement across the country.

Can I file my report over the phone?

If you're not able to use ReportFraud.ftc.gov to file a report, you can call the FTC's Consumer Response Center at 877-382-4357.

Can I file a report in another language?

To file your report in Spanish, go to ReporteFraude.ftc.gov.

To report in languages other than English and Spanish, call [877-382-4357](tel:877-382-4357) from 9 am to 5 pm ET. Press 3 for a list of languages, and then 0 for more languages.

What does the FTC do with my personal information?

Protecting the privacy and security of consumers' personal information is very important to us. Learn more about what the FTC does with the information you give us at ftc.gov/site-information/privacy-policy. Giving us your contact information can help if we need more information, but how much information you share is up to you.

Can I file my report anonymously?

Yes, you can file a report anonymously. You also can give as much or as little information as you want. It's helpful to have contact information in case the FTC needs to learn more about your experience.

[Start your report now.](#)

Yes, you can file a report anonymously. You also can give as much or as little information as you want. It's helpful to have contact information in case the FTC needs to learn more about your experience.

[Start your report now.](#)

After I file a report

What happens to my report?

Your report goes into the FTC's Consumer Sentinel database, which is available to federal, state, and local law enforcement across the country.

The FTC uses reports like yours to investigate and bring cases against fraud, scams, and bad business practices. The FTC can't resolve reports on behalf of individuals. But the FTC also makes reports available to more than 2,800 law enforcement partners.

The FTC also uses reports to spot trends, educate the public, and share data about what's happening in your community. You can see what's going on in your state or metro area by visiting ftc.gov/exploredata.

When the FTC brings cases, we try to get money back for people. At ftc.gov/refunds, you can see recent FTC cases that resulted in refunds.

Watch [this video](#) to learn about the importance of reporting to the FTC.

Will I hear back from the FTC?

The FTC is not able to respond to each report individually, and it can't take action on behalf of individual consumers. The FTC uses reports like yours to investigate and bring cases against fraud, scams, and bad business practices. Each year, the FTC brings hundreds of law enforcement cases. We'll also make your

Will I hear back from the FTC?

The FTC is not able to respond to each report individually, and it can't take action on behalf of individual consumers. The FTC uses reports like yours to investigate and bring cases against fraud, scams, and bad business practices. Each year, the FTC brings hundreds of [law enforcement cases](#). We'll also make your report available to more than 2,800 law enforcement partners.

When you submit your report, we'll offer you next steps you can take to protect yourself or recover from fraud. If you include your email address in your report, we'll also send you an email with these steps.

Will the FTC call me?

Typically, no. If the FTC ever does call you about a report you filed, the person calling will have the reference number you were given for your report when you submitted it. If anyone calls for any other reason saying they're from the FTC, that's probably a scammer.

Scammers are impersonating the FTC. Know that the FTC will never threaten you, say you must transfer your money or deposit money in a cryptocurrency ATM to "protect it," or tell you to withdraw cash or buy gold and give it to someone. The FTC does not give out sweepstakes prizes. Learn more at ftc.gov/impersonators.

If you believe you received a call from an FTC employee, you can call the FTC at (202) 326-2000 to check it out.

Can I find out what's happened with my report?

The FTC can't give updates on reports that have been filed or respond to each report individually. If the FTC files an enforcement action and gets money back for people, the agency will try to contact those who lost money.

Each year, the FTC brings hundreds of law enforcement cases. Learn about the cases with active refund

The FTC can't give updates on reports that have been filed or respond to each report individually. If the FTC files an enforcement action and gets money back for people, the agency will try to contact those who lost money.

Each year, the FTC brings hundreds of [law enforcement cases](#). Learn about the cases with active refund programs at [ftc.gov/refunds](#).

Can I update my report?

If you have additional information to share, you can file a new report at [ReportFraud.ftc.gov](#). You can include your prior report number, if you have it, in the comments.

Can I get a copy of my report or report number?

When you submit your report, you'll have the chance to print or save a copy. The report will include the report number. If you leave the page without printing or saving, you won't be able to get a copy of your report.

If you gave us your email address, you'll get an email with your report number and next steps to take, but the email won't include the report itself.

If you need a copy of your unsaved report, you can file a Freedom of Information Act request at [ftc.gov/foia/make-foia-request](#) or submit a new report.

Should I file a report with anyone else?

Your report goes into Consumer Sentinel, a database available to federal, state, and local law enforcement across the country. But you also can file a report with other agencies, including your [state attorney general](#) or [local consumer protection agency](#).

Your report goes into Consumer Sentinel, a database available to federal, state, and local law enforcement across the country. But you also can file a report with other agencies, including your [state attorney general](#) or [local consumer protection agency](#).

Will unwanted calls stop if I report them?

Reporting unwanted calls won't instantly stop them. But reporting does matter. The FTC analyzes report data and trends to identify illegal callers based on calling patterns.

The FTC takes the phone numbers you report and releases them to the public each business day. This helps phone carriers and others working on call-blocking and call-labeling solutions. Your reports also help law enforcement identify the people behind illegal calls.

To get fewer illegal robocalls, look into call-blocking and call-labeling solutions. The call-blocking option you choose will depend on whether you're getting calls on a cell phone, traditional landline, or home phone that uses the internet (VoIP). Learn more at ftc.gov/calls.

Will the FTC share my information with the company I'm reporting?

We won't automatically share your information with the company, but [there are times](#) when we may need to share it — for example, if a judge orders us to. If you prefer, you can submit your report anonymously. Including your contact information can help if the FTC needs more information from you, but it's not required. [Start your report now](#).

How can I stay connected with the FTC to learn about new scams?

Stay connected by [signing up](#) for the FTC's Consumer Alerts. You'll get periodic emails with advice and scam alerts from the FTC. To see recent Consumer Alerts go to ftc.gov/scams.

Stay connected by [signing up](#) for the FTC's Consumer Alerts. You'll get periodic emails with advice and scam alerts from the FTC. To see recent Consumer Alerts go to ftc.gov/scams.

Getting my money back

How do I get my money back?

After you file your report, we will give you steps to take that could help as you try to get your money back or stop a charge, depending on how you paid. The quicker you act, the better your chance of getting your money back. You also can find that information at ftc.gov/scams.

In some cases, an FTC law enforcement action gets money back to people. To see recent FTC cases that resulted in refunds, go to ftc.gov/refunds. But if someone tells you to send money to get a refund from the FTC or any other government agency, it's a scam.

What can I do if I paid a scammer with a gift card?

If you bought a gift card and gave a scammer the numbers:

- **Contact the company that issued the gift card right away.** Use this [list of contacts](#). Tell them the card was used in a scam and ask for your money back.
 - **Try to find your receipt from when you bought the gift card and the card itself.** It could help you recover your money from the gift card company.
 - **Learn more at** ftc.gov/giftcards.
-

What can I do if I paid a scammer with a wire transfer?

If you paid a scammer with a wire transfer:

Source URL: <https://reportfraudftcgov.netlify.app/faq>

Collection Timestamp: Wed Sep 02 2026 12:20:30 GMT+0000 (UTC)

What can I do if I paid a scammer with a wire transfer?

If you paid a scammer with a wire transfer:

- **Contact the bank or company that did the wire transfer right away.** If you used a money transfer company, call them immediately to file a fraud complaint. Call the complaint department:
 - MoneyGram at **1-800-MONEYGRAM (1-800-666-3947)**
 - Western Union at **1-800-325-6000**
- **Ask for the wire transfer to be reversed.** It's unlikely to happen, but it's important to ask.

What can I do if I paid a scammer with a credit or debit card?

If you paid a scammer with a credit or debit card:

1. **File a dispute (also called a "chargeback") with your credit or debit card company.**
 - **Online:** Log onto your credit or debit card company's website and go through the dispute process.
 - **By Phone:** Call the phone number on the back of your card and tell them why you're filing a dispute.
2. **Follow up with a letter to your credit or debit card company.** To protect any rights you may have, follow up in writing by sending a letter to the address listed for billing disputes or errors. [Use our sample letter.](#)
3. **Save your records.** Keep any letters, notes, or emails related to the scam — they could help prove you're entitled to a refund if the credit or debit card company has any questions.
4. **Find out your rights at ftc.gov/credit.**

How do I dispute an electronic bank transfer?

If you paid with an electronic bank transfer or withdrawal:

- **Contact your bank immediately.** Ask if the bank can stop the transaction or recover your money from

How do I dispute an electronic bank transfer?

If you paid with an electronic bank transfer or withdrawal:

- **Contact your bank immediately.** Ask if the bank can stop the transaction or recover your money from the person's or company's account. Tell the bank the reason you want to stop the transfer, and give them the bank account number your money was sent to. Don't wait. Let your bank know as soon as you can.
 - **If the bank won't help you, file a complaint with the CFPB at consumerfinance.gov/complaint.**
-

How do I stop a payment that I mailed?

If you sent cash by U.S. mail:

- **Contact the U.S. Postal Inspection Service at 877-876-2455.**
 - **Ask the U.S. Postal Service to "intercept" the package.** To learn more about this process, visit <https://faq.usps.com/s/article/USPS-Package-Intercept-The-Basics>.
 - **Otherwise, contact whatever delivery service you used as soon as possible.**
-

How do I stop a money order?

To stop payment on a money order:

- **Contact the company that issued the money order right away.** See if you can stop payment.
 - **Next, try to stop delivery of the money order.** If you sent it by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455. Ask the U.S. Postal Service to "intercept" the package. To learn more about this process, visit <https://faq.usps.com/s/article/USPS-Package-Intercept-The-Basics>. Otherwise, contact whatever delivery service you used as soon as possible.
-

What can I do if I didn't get a product or service I paid for?

Source URL: <https://reportfraudftcgov.netlify.app/faq>

Collection Timestamp: Wed Sep 02 2026 12:20:30 GMT+0000 (UTC)

Otherwise, contact whatever delivery service you used as soon as possible.

What can I do if I didn't get a product or service I paid for?

Try contacting the seller first to resolve the problem and get a refund. Most legitimate businesses want to keep you happy so you'll keep coming back.

If that doesn't work, you can use these tips to try to reverse the charge or get your money back, depending on how you paid:

- [Credit or debit card](#)
- [Electronic bank transfer or withdrawal](#)
- [Wire transfer](#)

What do I do if I gave someone personal information like my Social Security number or passwords?

If you think a scammer has your information, like your Social Security, credit card, or bank account number:

- Go to [IdentityTheft.gov](https://www.identitytheft.gov). Look for specific steps to take based on the information that was stolen.

If you gave your username and password to a scammer:

- **Change your password right away.** If you use the same password for other accounts or sites, change it there, too. [Create a new password that is strong.](#)

If someone calls and offers to "help" you recover money you have already lost:

- **Don't give them money or personal information.** [You're probably dealing with a fake refund scam.](#)

Learn more about different scams and how to recover from them at [ftc.gov/scams](https://www.ftc.gov/scams).

- Don't give them money or personal information. [You're probably dealing with a fake refund scam.](#)

Learn more about different scams and how to recover from them at ftc.gov/scams.

What do I do if I paid a scammer with cryptocurrency?

If you paid a scammer with cryptocurrency:

While it is very difficult to get your money back when you pay using cryptocurrency, you can try to contact the company you used to send the money and tell them it was a fraudulent transaction. Ask to have the transaction reversed, if possible.

Scams

How can I find out if something is a scam?

Here are some ways you can tell you're dealing with a scam:

- **Scammers usually pressure you to act quickly.** They don't want you to have time to check what they're saying.
- **Scammers tell you to pay in a specific way.** They want it to be hard to get your money back, so they'll say to pay by gift card, by wire transfer, or with cryptocurrency.
- **Scammers ask for your personal or financial information** — things like your Social Security, credit card, or bank account number.

Before you act, type the company or product name into your favorite search engine with terms like “review,” “complaint,” or “scam,” and see what you find.

For more on how to recognize a scam, go to ftc.gov/scams.

Before you act, type the company or product name into your favorite search engine with terms like “review,” “complaint,” or “scam,” and see what you find.

For more on how to recognize a scam, go to ftc.gov/scams.

How do I know if a call is from a scammer?

Scammers who call you have a few things in common:

- They'll ask for money or information (like your Social Security, credit card, or bank account number)
- They'll tell you how to pay — often by gift card, cryptocurrency, or wire transfer.

And remember: caller ID can be faked. So even if it looks like the call comes from a government agency like the Social Security Administration, IRS, or Medicare, or looks like it comes from a local number, it could be a scammer calling from anywhere in the world. Learn more about the signs of a scam at ftc.gov/scams.

How can I find out if a company I want to do business with is legitimate?

If you're thinking about dealing with a company you don't know, do some research first. Anyone can put up a website under almost any name. So before you buy, invest, or otherwise deal with a company, confirm their physical address and phone number in case you have questions or problems later.

Then type the company's name into your favorite search engine with terms like “review,” “complaint,” or “scam” to see what people have to say about them.

Finally, learn the signs of a scam at ftc.gov/scams.

I received a check or claim form from the FTC — is it real?

A check or claim form sent as part of an FTC settlement will include an explanation and details about the case. Review recent cases that resulted in refunds at ftc.gov/refunds. If someone tells you to send money

I received a check or claim form from the FTC — is it real?

A check or claim form sent as part of an FTC settlement will include an explanation and details about the case. Review recent cases that resulted in refunds at ftc.gov/refunds. If someone tells you to send money to get a refund from the FTC or any other government agency, it's a scam.

Did the FTC call me?

If the FTC ever does call you about a report you filed as part of a possible investigation, the person calling will have the reference number you were given for your report when you submitted it. If anyone calls for any other reason, saying they're from the FTC, that's probably a scammer. We've heard reports of fake FTC callers, sometimes claiming to have refunds or prize winnings, and asking you to pay a fee to get them. That's a scam. **The FTC will never ask you to send money for any reason.** Learn more about the signs of a scam at ftc.gov/scams.

If you believe you received a call from an FTC employee, call the FTC at (202) 326-2000.

How can I avoid a cryptocurrency scam?

Scammers are always finding new ways to steal your money using cryptocurrency. **One sure sign of a scam is anyone who says you have to pay by cryptocurrency.** In fact, anyone who tells you to pay by [wire transfer](#), [gift card](#), or [cryptocurrency](#) is a scammer. Of course, if you pay, there's almost no way to get that money back. Which is what the scammers are counting on. Common cryptocurrency scams include investment and business opportunity scams, blackmail emails, and social media scams. Learn more at ftc.gov/cryptocurrency.

How can I avoid an Amazon impersonator scam?

Scammers are calling people and using the name of a company everyone knows, Amazon, to rip people off.

How can I avoid an Amazon impersonator scam?

Scammers are calling people and using the name of a company everyone knows, Amazon, to rip people off.

In one version of the scam, you get a call and a recorded message that says it's Amazon. The message says there's something wrong with your account. It could be a suspicious purchase, a lost package, or an order they can't fulfill.

If you get an unexpected call or message about a problem with any of your accounts, hang up.

- Do not press '1' to speak with customer support
- Do not call a phone number they gave you
- Do not give out your personal information

If you think there may actually be a problem with one of your accounts, contact the company using a phone number or website you know is real.

If you believe you are dealing with a scammer, you can use our [online form](#) to file a report about your issue if you haven't already.

Click [here](#) to learn more about impersonator scams.

How can I avoid a government impersonator scam?

You've gotten the calls: from Social Security. Or the IRS. Or Medicare. Or any number of other agencies. Except: as soon as the caller threatens you or demands that you pay them with a gift card or by wiring money, you know. It's a scam. Even if caller ID tells you otherwise – that's not the government calling.

© 2025 ReportFraud.gov. All rights reserved. | Privacy Policy | Terms of Service

you've gotten the calls: from Social Security. Or the IRS. Or Medicare. Or any number of other agencies. Except: as soon as the caller threatens you or demands that you pay them with a gift card or by wiring money, you know. It's a scam. Even if caller ID tells you otherwise – that's not the government calling.

Government imposters may call to "verify your Social Security number," or say your Social Security number or Medicare benefits have been "suspended" due to a mix-up. Scammers may say your tax returns must be done differently because of a name change — and they need your Social Security number to fix it. For recently married people, or a trans person who recently changed their name, the excuses scammers use might make sense. But wait right there. Scammers are just phishing for personal information they can use to steal your identity or take your money.

So how do you spot it and stop it? Here's what to know:

- **Scammers call, email, or text you for money or information.** But the government won't. Anyone who calls, emails, or texts, asking for money or personal information and claims to be from the government is a scammer. Hang up and don't respond to messages.
- **Scammers tell you how to pay — usually by wiring money, cryptocurrency, or gift card.** Nobody legit will **ever** tell you to pay in any of those ways. If they call, hang up the phone. If they email, text, or message you, don't click on any links. It's a scam.
- **Even if your caller ID says it's from the government, it could be a scam.** Caller ID can be faked. Even if it shows the government agency's real phone number, or even if it says something like "Social Security Administration," it could be anyone calling from anywhere in the world. Don't trust it.

People are telling the FTC that they're getting calls from — and losing money to — scammers pretending to be the Social Security Administration, IRS, Medicare, a government grants group, or cops and the FBI.

If you believe you are dealing with a scammer, you can use our [online form](#) to file a report about your issue if you haven't already.

Click [here](#) to learn more about impersonator scams.

issue if you haven't already.

Click [here](#) to learn more about impersonator scams.

How can I avoid a fake check scam?

If someone you don't know sends you a check and asks for money back, that's a scam.

Fake checks come in many forms. They might look like business or personal checks, cashier's checks, money orders, or electronic checks. Here's what you need to know about fake check scams.

In a fake check scam, a person you don't know asks you to deposit a check — sometimes for several thousand dollars, and usually for more than you are owed — and send some of the money back, to them or another person. The scammers always have a good story to explain the overpayment. They might say they're stuck out of the country, they need you to cover taxes or fees, you'll need to buy supplies, or something else.

If you believe you are dealing with a scammer, you can use our [online form](#) to file a report about your issue if you haven't already.

Click [here](#) to learn more about fake check scams.

How can I avoid a phishing scam?

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

Scammers often update their tactics, but there are some signs that will help you recognize a phishing

try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like these every day — and they're often successful.

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- want you to click on a link to make a payment
- say you're eligible to register for a [government](#) refund
- offer a coupon for free stuff

If you believe you are dealing with a scammer, you can use our [online form](#) to file a report about your issue if you haven't already.

How can I avoid a robocall scam?

It's cheap and easy for scammers and telemarketers to make robocalls over the internet from anywhere in the world. If someone is already breaking the law by robocalling you without permission, there's a good chance it's a scam. At the very least, it's a company you don't want to do business with. Don't rely on your caller ID. Scammers can fake the name and number that shows up, making it look like a call is from a

It's cheap and easy for scammers and telemarketers to make robocalls over the internet from anywhere in the world. If someone is already breaking the law by robocalling you without permission, there's a good chance it's a scam. At the very least, it's a company you don't want to do business with. Don't rely on your caller ID. Scammers can fake the name and number that shows up, making it look like a call is [from a government agency like Medicare](#) or a local number. That's called spoofing.

You can watch out for common phone scams like [government impersonator scams](#) . If someone calls you out of the blue and asks you to hand over personal information or [wire money](#) or [pay with a gift card](#) , it's a scam.

If you believe you are dealing with a scammer, you can use our [online form](#) to file a report about your issue if you haven't already.

How can I avoid a spam text message scam?

Scammers send fake text messages to trick you into giving them your personal information – things like your password, account number, or Social Security number. If they get that information, they could gain access to your email, bank, or other accounts. Or they could sell your information to other scammers. The scammers use a variety of ever-changing stories to try to rope you in. They may

- promise free prizes, [gift cards](#) or coupons
- offer you a low or no interest credit card
- promise to help you pay off your student loans

Scammers also send fake messages that say they have some information about your account or a transaction. The scammers may

- say they've noticed some suspicious activity on your account
- claim there's a [problem with your payment information](#)
- send you a [fake invoice](#) and tell you to contact them if you didn't authorize the purchase

transaction. The scammers may

- say they've noticed some suspicious activity on your account
- claim there's a [problem with your payment information](#)
- send you a [fake invoice](#) and tell you to contact them if you didn't authorize the purchase
- send you a [fake package delivery notification](#)

If you believe you are dealing with a scammer, you can use our [online form](#) to file a report about your issue if you haven't already.

Click [here](#) to learn more about spam text messages.

What you can do

Where can I learn more about scams and my rights as a consumer?

Go to consumer.ftc.gov. You'll find articles, blog posts, videos, and infographics on a range of consumer topics.

What should I do if I lost money to a scam?

Once you send money to a scammer, it's often gone. But it is sometimes possible to get your money back.

- [If you paid with a credit or debit card, try disputing the charge right away.](#)
- [If you paid with a gift card, contact the gift card company right away.](#)
- [If you paid with a wire transfer, immediately contact Western Union, MoneyGram, or whatever company you used.](#)
- If you mailed cash or a money order, try to stop the delivery. You can also try to stop payment on a

Source URL: <https://reportfraudftcgov.netlify.app/faq>

Collection Timestamp: Wed Sep 02 2026 12:20:30 GMT+0000 (UTC)

- [If you paid with a gift card, contact the gift card company right away.](#)
- [If you paid with a wire transfer, immediately contact Western Union, MoneyGram, or whatever company you used.](#)
- [If you mailed cash or a money order, try to stop the delivery. You can also try to stop payment on a money order.](#)
- [If you paid with an electronic bank transfer or withdrawal, contact your bank immediately.](#)

For more tips on what to do, visit ftc.gov/scams.

Where can I find information on a specific FTC rule or act?

The FTC enforces federal consumer protection laws that prevent fraud, deception, and unfair business practices. The FTC also enforces federal antitrust laws that prohibit anticompetitive mergers and other business practices that could lead to higher prices, fewer choices, or less innovation.

These laws, regulations, and trade rules include the Federal Trade Commission Act, Telemarketing Sales Rule, Identity Theft Act, Fair Credit Reporting Act, and Clayton Act. In total, the Commission has enforcement or administrative responsibilities under more than 70 laws. Learn more at ftc.gov/enforcement. And for more on how these rules might apply to you, go to consumer.ftc.gov.

What can I do about robocalls and other annoying calls?

To get fewer illegal robocalls, look into call-blocking and call-labeling solutions. The call-blocking option you choose will depend on whether you're getting calls on a cell phone, traditional landline, or home phone that uses the internet (VoIP).

The FTC analyzes complaint data and trends to identify illegal callers based on calling patterns. The FTC takes the phone numbers you report and releases them to the public each business day. This helps phone carriers and others that are working on call-blocking solutions. Your reports also help law enforcement identify the people behind illegal calls.

The FTC analyzes complaint data and trends to identify illegal callers based on calling patterns. The FTC takes the phone numbers you report and releases them to the public each business day. This helps phone carriers and others that are working on call-blocking solutions. Your reports also help law enforcement identify the people behind illegal calls.

If you're getting a lot of robocalls, they're probably scams. Learn more at ftc.gov/calls.

What do I do if I think my computer has malware because of a tech support scam?

If you gave a scammer remote access to your computer:

- **Update your computer's security software.**
- **Run a scan and delete anything it identifies as a problem.**
- **If you shared any passwords, change them right away.** If you use the same password for other accounts or sites, change it there, too. [Create new passwords that are strong.](#)
- **If you think there's a problem with your computer, find a computer technician you can trust.** Try finding someone at your computer manufacturer's website or a store that sells computer equipment and offers technical support in person.

How can I tell if a check is real or part of a fake check scam?

In a fake check scam, a person you don't know asks you to deposit a check and send some of the money to another person. If you deposit the fake check, the check might "clear" and the funds might become available. You might think it's safe to send the money — but it's not. By law, banks have to make deposited funds available quickly, usually within two days. But that doesn't mean it's a good check. Fake checks can take weeks to be discovered and untangled. By that time, the scammer has any money you sent, and you're stuck paying the money back to the bank.

Since it's not always easy to tell whether a check is fake, don't rely on money from a check unless you know and trust the person you're dealing with. Learn more at consumer.ftc.gov

you're stuck paying the money back to the bank.

Since it's not always easy to tell whether a check is fake, don't rely on money from a check unless you know and trust the person you're dealing with. Learn more at consumer.ftc.gov

Also see: [I received a check or claim form from the FTC — is it real?](#)

Do you have advice for business owners?

Yes, at ftc.gov/business, your link to consumer protection law. You'll find guidance for business and legal resources, including advice for [small business](#).

How can I share this website with people I know?

You'll find graphics and videos you can share on social media or add to your website at ReportFraud.ftc.gov/partners. Thank you for helping to fight fraud in your community by telling others about ReportFraud.ftc.gov.

ReportFraud.ftc.gov is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

[Privacy Policy](#)



FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

[FAQs](#)

[Español](#)

Source URL: <https://reportfraudftcgov.netlify.app/faq>

Collection Timestamp: Wed Sep 02 2026 12:20:30 GMT+0000 (UTC)

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

[Privacy Policy](#)

[FAQs](#)

[Español](#)

[Report Now](#)

OMB CONTROL#: 3084-0169
Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.

Source URL: <https://reportfraudftcgov.netlify.app/faq>
Collection Timestamp: Wed Sep 02 2026 12:20:30 GMT+0000 (UTC)



FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

Start



Submit

Is your report about any of these common problems?

Choose the best fit. If you don't see your problem, choose "Something else."

An impersonator (ex. fake government, business, love interest, grandchild)	Online shopping
Job, investment, money-making opportunity, franchise	Sweepstakes, prize, lottery
Phone, internet, TV service	Auto sale, repair
Health (ex. weight loss, eye care, treatment)	Credit, debt, loan (ex. debt collection, credit report, student loan debt relief)
Just an annoying call	Something else (we'll get it to the right place)

Continue →

Source URL: <https://reportfraudftcgov.netlify.app/assistant>

Collection Timestamp: Wed Sep 02 2026 12:22:48 GMT+0000 (UTC)

Health
(ex. weight loss, eye care, treatment)

Credit, debt, loan
(ex. debt collection, credit report, student loan debt relief)

Just an annoying call

Something else
(we'll get it to the right place)

Continue →

ReportFraud.ftc.gov is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

[Privacy Policy](#)



FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

[FAQs](#)

[Report Now](#)

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.

Source URL: <https://reportfraudftcgov.netlify.app/assistant>

Collection Timestamp: Wed Sep 02 2026 12:22:48 GMT+0000 (UTC)



FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

Start Submit

Report details

Please share as much as you know. The details help law enforcement investigations.

Did you pay or send money? ☒ Yes ☐ No

How much money did you pay or send?

\$

How did you pay or send the money?

Select

When did you most recently pay or send money (mm/dd/yyyy)?

How did it start (ex. how did they first contact you, where did you see an ad)?

Select

Source URL: <https://reportfraudftcgov.netlify.app/form/main>

Collection Timestamp: Wed Sep 02 2026 12:25:01 GMT+0000 (UTC)

When did you most recently pay or send money (mm/dd/yyyy)?

How did it start (ex. how did they first contact you, where did you see an ad)?

Select

Details about the company or individual

Please share as much as you know. The details help law enforcement investigations.

Name of the company

Name of the person you dealt with

Their First Name

Their Last Name

Do you have any other information about them (phone, website, etc.)?

☐ Yes

☒ No

Comments

Describe what happened.
Tell us what happened in your own words. Include specific details you remember.
Do not include any sensitive information, such as SSN, DOB, driver's license numbers, account numbers, medical history, etc.

Describe what happened.

Tell us what happened in your own words. Include specific details you remember.

Do not include any sensitive information, such as SSN, DOB, driver's license numbers, account numbers, medical history, etc.

0 characters of 3500 used



Blue Left Arrow Back

Continue →

[ReportFraud.ftc.gov](https://reportfraud.ftc.gov) is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

[Privacy Policy](#)



FEDERAL TRADE COMMISSION
[ReportFraud.ftc.gov](https://reportfraud.ftc.gov)

[FAQs](#)

[Report Now](#)

OMB CONTROL#: 3084-0169

Source URL: <https://reportfraudftcgov.netlify.app/form/main>

Collection Timestamp: Wed Sep 02 2026 12:25:01 GMT+0000 (UTC)

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.

Source URL: <https://reportfraudftcgov.netlify.app/form/main>

Collection Timestamp: Wed Sep 02 2026 12:25:01 GMT+0000 (UTC)



FEDERAL TRADE COMMISSION
ReportFraud.ftc.gov

Start Submit

About you

Are you filing this report for someone else? ☐ Yes ☒ No

Your details

First Name

Last Name

Country or region

Select ▾

Street Address 1 (street address, PO Box)

Street Address 2 (apartment, suite, unit, building, floor)

City

State/Province/Region

Source URL: <https://reportfraudftcgov.netlify.app/form/main>

Collection Timestamp: Wed Sep 02 2026 12:26:04 GMT+0000 (UTC)

Country or region

Select

Street Address 1 (street address, PO Box)

Street Address 2 (apartment, suite, unit, building, floor)

City

State/Province/Region

Zip/Postal Code

Phone Number

Phone Type

Select

Email Address

Email address is required if you want an email confirming we have received your report.

Age Range

Select

Military Status

Select

Military Rank

Select

Military Branch

Select

Are you filing on behalf of your small business or organization?

☐ Yes ☒ No

Are you filing on behalf of your small business or organization?

☐ Yes

☒ No



Blue Left Arrow Back

Submit →

ReportFraud.ftc.gov is the federal government's website where you can report fraud, scams, and bad business practices.

Visit consumer.ftc.gov to find tips and learn how to avoid scams.

[Privacy Policy](#)



FEDERAL TRADE COMMISSION

ReportFraud.ftc.gov

[FAQs](#)

[Report Now](#)

OMB CONTROL#: 3084-0169

Under the Paperwork Reduction Act, federal agencies are not allowed to collect information from the public without a valid OMB control number.

Source URL: <https://reportfraudftcgov.netlify.app/form/main>

Collection Timestamp: Wed Sep 02 2026 12:26:04 GMT+0000 (UTC)