# Avoiding Identity Theft

Identity theft can make it hard for you to get credit, a job, a place to live, or utilities. But you can reduce your risk of being hurt by identity theft.

## How can I protect my identity?

Protect your personal information. That helps you protect your identity. Here are some things you can do:

- At home
  - keep your financial records, Social Security and Medicare cards in a safe place
  - shred papers that have your personal or medical information
  - take mail out of your mailbox as soon as you can
- As you do business
  - only give your Social Security number if you must. Ask if you can use another kind of identification
  - do not give your personal information to someone who calls you or emails you
- On the computer
  - use passwords that are not easy to guess. Use numbers and symbols when you can
  - do not respond to emails or other messages that ask for personal information
  - do not put personal information on a computer in a public place, like the library

## How will I know if someone steals my identity?

Read your bills and account statements. Watch for:

- things you did not buy
- withdrawals you did not make
- a change of your address that you did not expect
- bills that stop coming

# Avoiding Identity Theft

Look at medical statements. You might see charges you do not recognize. That might mean someone stole your identity.

Get your credit report. You get one free credit report every year from each credit reporting company. To order:

- Call Annual Credit Report at 1-877-322-8228.
- Answer questions from a recorded system. You have to give your address, Social Security number, and birth date.
- Choose to only show the last four numbers of your Social Security number. It is safer than showing the full number on your report.
- Choose which credit reporting company you want a report from. (You get one report free from each company every year.)

The company mails your report to you. It should arrive two to three weeks after you call.

Read your credit report carefully. Look for mistakes or accounts you do not recognize. This could mean someone stole your identity.

**If you spot a scam...**

Tell someone
Then tell the **FTC**

**ftc.gov/complaint**
1-877-FTC-HELP
(1-877-382-4357)

If you spot a scam, report it at
**ftc.gov/complaint**.

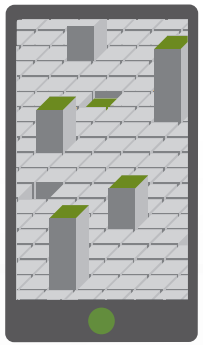
Your reports help the FTC and other law enforcement investigate scams and bring crooks to justice.

# 10 things you can do to AVOID FRAUD

**FEDERAL TRADE COMMISSION**
July 2016

**1 Spot imposters.** Scammers often pretend to be someone you trust, like a government official, a family member, a charity, or a company you do business with. Don't send money or give out personal information in response to an unexpected request – whether it comes as a text, a phone call or an email.

**2 Do online searches.** Type a company or product name into your favorite search engine with words like "review," "complaint" or "scam." Or search for a phrase that describes your situation, like "IRS call." You can even search for phone numbers to see if other people have reported them as scams.



**3 Don't believe your caller ID.** Technology makes it easy for scammers to fake caller ID information, so the name and number you see aren't always real. If someone calls asking for money or personal information, hang up. If you think the caller might be telling the truth, call back to a number you know is genuine.

**4 Don't pay upfront for a promise.** Someone might ask you to pay in advance for things like debt relief, credit and loan offers, mortgage assistance, or a job. They might even say you've won a prize, but first you have to pay taxes or fees. If you do, they will probably take the money and disappear. Learn where to get real help with these issues at **consumer.ftc.gov**.

**5 Consider how you pay.** Credit cards have significant fraud protection built in, but some payment methods don't. Wiring money through services like Western Union or MoneyGram is risky because it's nearly impossible to get your money back. That's also true for reloadable cards like MoneyPak, Reloadit or Vanilla. Government offices and honest companies won't require you to use these payment methods.

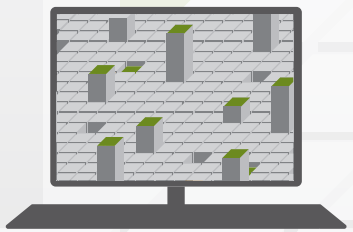
**6 Talk to someone.** Before you give up your money or personal information, talk to someone you trust. Con artists want you to make decisions in a hurry. They might even threaten you. Slow down, check out the story, do an online search, consult an expert — or just tell a friend.

**7 Hang up on robocalls.** If you answer the phone and hear a recorded sales pitch, hang up and report it to the FTC. These calls are illegal, and often the products are bogus. Don't press 1 to speak to a person or to be taken off the list. That could lead to more calls.

**8 Be skeptical about free trial offers.** Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and read the cancellation policy. And always review your monthly statements for charges you don't recognize.

**9 Don't deposit a check and wire money back.** By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. If a check you deposit turns out to be a fake, you're responsible for repaying the bank.

**10 Sign up for free scam alerts from the FTC at ftc.gov/scams.** Get the latest tips and advice about scams sent right to your inbox.



have you HEARD about...

# “You’ve Won” Scams

## Here’s how they work:

You get a card, a call, or an email telling you that you won! Maybe it’s a trip or a prize, a lottery or a sweepstakes. The person calling is so excited and can’t wait for you to get your winnings.

But here’s what happens next: they tell you there’s a fee, some taxes, or customs duties to pay. And then they ask for your credit card number or bank account information, or they ask you to wire money.

Either way, you lose money instead of winning it. You don’t ever get that big prize. Instead, you get more requests for money, and more promises that you won big.

## Here’s what you can do:

1. **Keep your money – and your information – to yourself.** Never share your financial information with someone who contacts you and claims to need it. And never wire money to anyone who asks you to.
2. **Pass this information on to a friend.** You probably throw away these kinds of scams or hang up when you get these calls. But you probably know someone who could use a friendly reminder.

Want to know more? Sign up for scam alerts at ftc.gov/subscribe.

...Pass it ON

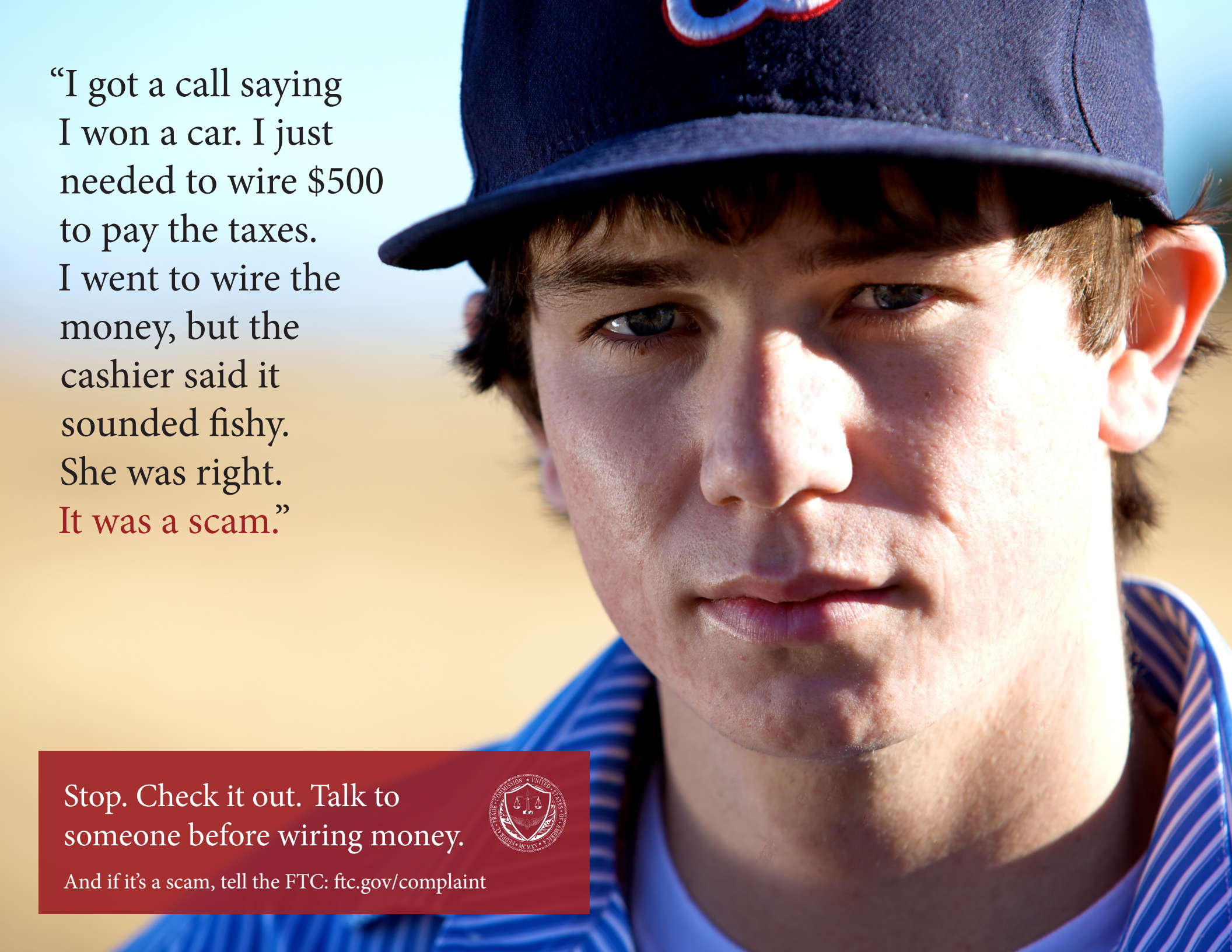
## Please Report Scams

If you spot a scam, please report it to the Federal Trade Commission.

- Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261
- Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the scammers and stop them before they can get someone's hard-earned money. It really makes a difference.


“My mom got a call saying, ‘Grandma, it’s your favorite grandson. I’m in New York and got into an accident. I need help. I need money.’
But he wasn’t in New York. It was a scam.”
Stop. Check it out. Talk to someone you trust before sending money.
Learn more about scams like this: ftc.gov/imposters


"I got a call saying I won a car. I just needed to wire $500 to pay the taxes. I went to wire the money, but the cashier said it sounded fishy. She was right. It was a scam."
Stop. Check it out. Talk to someone before wiring money.
And if it's a scam, tell the FTC: ftc.gov/complaint