IDENTITY THEFT

KEEP YOUR INFORMATION TO YOURSELF!

Identity thieves may already have a lot of information about you - like your credit card number, the card's expiration date, and your name, address, and phone number. With all that information in his hands, why would he call you? He's after one vital piece of information - the security code on your credit card.

Here's how the scam works. The scammer says he's calling from your credit card's security or fraud department. They've flagged some suspicious activity on your card, he says. He makes up a bogus transaction and asks if you authorized it. Of course, you didn't. So he says he'll open a fraud investigation, gives you a case reference number, and tells you to call the phone number on your credit card if you have any questions. It all seems fine so far, right?

But, he says, there's just one more thing. He needs to verify that you are in possession of the card - so he asks you to tell him the security code. And it's the final piece of the puzzle he's after.

If you get a call like this:

- **Don't give the caller any information about your account**—even if he already knows some of the details.
- **Hang up the phone.** Call the customer service number on the back of your credit card. Talk to the fraud or security department and ask about the unauthorized charges the caller told you about.
- **Report the suspicious call** to the FTC at ftc.gov/complaint or 1-877-FTC-HELP.
- **Tell your friends, family, neighbors, and others about it.** By spreading the word, you can help someone you care about avoid falling for a scam.

Identity thieves will try a lot of different tricks to get your personal information. No matter the story they tell you, don't give anyone your personal information if you didn't initiate the contact using contact information you know is trustworthy. And find out what else you can do to protect your personal information from ending up in the wrong hands.