Scams and Identity Theft

What to do if you become a victim.

Find out what to do if you suspect identity theft, gave money to someone you think is a scammer, gave a scammer your personal information, or access to your computer or phone.

Identity theft occurs when someone steals your identity to commit fraud. Stealing your identity could mean using personal information without your permission, such as, your name, Social Security number, or credit card number. You may not know about the theft until you review your credit report, credit card statement, or until you're contacted by a debt collector.

How can I spot identity theft?
Keep an eye out for identity theft by checking your credit card or bank statements and free credit reports from each of the three major credit bureaus at least once a year. If an identity thief is opening financial accounts in your name, these accounts may show up on your credit report.

You suspect your identity has been stolen, now what?

How do I report identity theft?

Contact:

- The Federal Trade Commission (FTC) online at IdentityTheft.gov or call 1-877-438-4338
- The three major credit reporting agencies and ask them to place fraud alerts and a credit freeze on your accounts.
- The fraud department at your credit card issuers, bank, and other places where you have accounts.
- Call or go into your local police department to file a report if needed.

How To Get Your Free Annual Credit Reports

The three nationwide credit bureaus, Equifax, Experian, and TransUnion — have a centralized website, toll-free telephone number, and mailing address so you can order your free annual reports in one place.

Visit: AnnualCreditReport.com
Call: 1-877-322-8228, or
complete the Annual Credit Report Request Form and mail it to:
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

Resources

Federal Trade Commission:
FTC.gov

Consumer Financial Protection Bureau:
Consumerfinance.gov

Identity Theft Resouces Center:
Idtheftcenter.org
888-400-5530

Non-Emergency Dispatch: 208-377-6790

Meridian Police: 208-888-6678

In person: M-F 8am-5pm
1401 E Watertower St. Meridian

You've been scammed, now what?

Scammers can be very convincing. They call, email, and send us text messages trying to get our money or sensitive personal information — like our Social Security or account numbers. Scammers are good at what they do.

If You Paid a Scammer:

Did you pay with a credit card or debit card, or authorize a bank transfer?
Contact the company or bank that issued the credit card or debit card. Tell them it was a fraudulent charge or transfer. Ask them to reverse the transaction and give you your money back.

Did you pay with a gift card?
Contact the company that issued the gift card. Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt. Companies will not typically refund your money.

Did you send a wire transfer through a company like Western Union or through your bank?
Contact the wire transfer company or bank. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

Did you send money through a money transfer app?
Report the fraudulent transaction to the company behind the money transfer app and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.

Did you pay with cryptocurrency?
Cryptocurrency payments typically are not reversible. Once you pay with cryptocurrency, you can only get your money back if the person you paid sends it back. But contact the company you used to send the money and tell them it was a fraudulent transaction. Ask them to reverse the transaction, if possible.

Did you send cash?
If you sent cash by U.S. mail, contact the U.S. Postal Inspection Service and ask them to intercept the package.

If You Gave a Scammer Your Personal Information:

Did you give a scammer your Social Security number?
Go to IdentityTheft.gov to see what steps to take, including how to monitor your credit.

Did you give a scammer your username and password?
Create a new, strong password. If you use the same password anywhere else, change it there too.

If a Scammer Has Access to Your Computer or Phone:

Does a scammer have remote access to your computer?
Update your computer's security software, run a scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information.

Did a scammer take control of your cell phone number and account?
Contact your service provider to take back control of your phone number. Once you do, change your account password. Also check your credit card, bank, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution.