



# Identity Theft

## What to know.

We're here to help:

For credit cards, call **1-800-955-9060**

For personal banking, call **1-800-935-9935**

For auto financing, call **1-800-336-6675**

For home lending, call **1-800-848-9136**

For more details, visit: [chase.com/securitycenter](https://chase.com/securitycenter)



### What is it?

Identity theft is when someone gets your personal information and uses it to commit fraud.

Pretending to be you, they could:

- Commit other crimes
- Open new credit cards in your name
- Steal money from your accounts
- Rent apartments
- Apply for loans



### What to look for.

- Unexplained transactions on credit cards or bank accounts
- New credit cards or financial accounts you didn't apply for
- Unexpected denial of a credit application
- Expected mail or emails are not received
- Unfamiliar inquiries on your credit report, calls from debt collectors or denial of an application you didn't submit
- A surprise drop in credit score
- Unusual activity on your Social Security account



### How it happens.

#### **Phishing** (pronounced "fishing") or **Smishing**

This is when fraudsters send reputable-looking emails or text messages trying to trick you into providing personal information or infecting your device with malware.

#### **Hacking**

This is when a thief gains access to your personal information by using technology to break into your computer, devices or network.

#### **Spoofing**

These are bogus websites or phone numbers that look legitimate and ask you to provide personal information.

#### **Stealing**

A thief takes your mail, personal documents, financial statements, laptop, smartphone or other device.



### How to help minimize the risk.

- Be vigilant with your documents, devices and property.
- Never provide your personal information to someone who calls, texts or emails you.
- At minimum, have unique passwords for your financial accounts and don't use them across multiple sites.
- Regularly check your credit report to monitor for changes you didn't anticipate.
- Sign up for free credit score and identity monitoring with Chase Credit Journey® and get alerts for changes to your credit report or if your info is found on the dark web at [chase.com/creditjourney](https://chase.com/creditjourney)
- Consider reaching out to the three credit bureaus for tools to protect your credit report or credit score.
- Never click any links or attachments in suspicious emails. If you're unsure it's legitimate, go to the organization's website directly.
- Only carry what you need (and never your Social Security card), in case of loss or theft.



We're here to help:

For credit cards, call **1-800-955-9060**

For personal banking, call **1-800-935-9935**

For auto financing, call **1-800-336-6675**

For home lending, call **1-800-848-9136**

For more details, visit: [chase.com/securitycenter](https://chase.com/securitycenter)

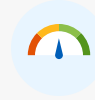
# Identity Theft

What to do if you believe your identity has been stolen.



## Notify the relevant companies or banks

- Get in touch with the relevant companies or banks immediately to alert them to the problem.
- Dispute the activity you believe to be fraudulent with them.



## Contact all three credit bureaus to review activity

- Obtain credit reports from the three bureaus to look for fraud. If you suspect fraud, notify all three credit bureaus to investigate and resolve the activity. Consider adding a freeze or fraud alert. A fraud alert will notify others that you might be a victim of fraud, while a freeze prevents the use of your credit without your approval.

### Equifax:

800-525-6285 | [equifax.com](https://equifax.com)

### Experian:

888-397-3742 | [experian.com](https://experian.com)

### TransUnion:

888-909-8872 | [transunion.com](https://transunion.com)



## Reach out to local law enforcement

- Supply all the information you can, including exact dates, times and account numbers.
- File a police report if advised.
- Save a copy of the police report because some businesses or financial institutions may require it to remove any fraudulent charges.



## Report your identity theft to the Federal Trade Commission

- The FTC is dedicated to protecting U.S. consumers.
- Go to their website, [identitytheft.gov](https://identitytheft.gov), to file a report, and get a recovery plan.
- When you file a report, the FTC and other agencies use your information to build cases against scammers.



## Tighten up your security

- Change the user names and passwords on all of your active accounts. Have unique passwords for your financial accounts, and don't use them across multiple sites. Consider using a password manager to create and store strong passwords.
- Keep your phone, computer and web browsers current, as there are often security patches included with system updates.
- On sites that offer it, use multifactor authentication as it requires more than just a password to log in.

