

Identity Theft Toolkit

WHAT YOU NEED TO DO

.....

This Toolkit is meant to serve as a guide to consumers who are victims of identity theft. The steps enclosed are general and apply to most identity theft situations. You may need to take additional steps to resolve your specific issue(s).

PAGE

1-2

STOPPING THE
DAMAGE

PAGE

1-3

REPAIRING THE
DAMAGE

PAGE

4

DAMAGE
CONTROL

STOP THE DAMAGE

Struggling with an identity theft event? Start here to minimize the damage.

1 REQUEST YOUR CREDIT REPORT:

WHAT IS IT? You are entitled to a **FREE** credit report from each credit reporting agency annually. Review them carefully for signs of identity theft. (i.e. accounts you didn't open, names/addresses that are not yours, etc.)

WHO DO I CONTACT? Call (877) 322-8228 or visit annualcreditreport.com to request your free credit reports.

WARNING! Beware of impostor websites or phone numbers. If you are asked for a credit card number, hang up or close the browser and try again.

2 PLACE A FRAUD ALERT

2 PLACE A FRAUD ALERT

WHAT IS IT? Federal law gives consumers the right to place a fraud alert on credit reports for **FREE**. It alerts potential creditors pulling your report to take extra steps to verify your identity before issuing credit or services in your name.

HOW LONG WILL IT LAST? One year. The alert allows you another free credit report from each of the three credit reporting agencies. While an initial fraud alert can be renewed, if you have proof you are a victim of identity theft, you can place an extended fraud alert that lasts seven years. *See page 4 for more information on the extended fraud alert.

WHO DO I CONTACT? You only have to contact one of the agencies and they'll notify the other two.
Equifax • (800) 685-1111 or equifax.com/personal/credit-report-services
Experian • (888) 397-3742 or experian.com/help
TransUnion • (800) 680-7289 or transunion.com/credit-help

3 CONSIDER A SECURITY FREEZE

WHAT IS IT? When a freeze is in place, a business that receives an application for products or services cannot access your credit report without your permission. Utilities, credit cards and insurance all commonly require a credit check. A freeze doesn't affect your existing lines of credit but will need to be thawed if you decide to apply for new credit or services. It is **FREE** to place, thaw or lift the freeze.

HOW LONG DOES IT LAST? The freeze lasts until **YOU** lift it. You can lift for a specified amount of time. After the time has elapsed, the freeze will go back into place. It can also be lifted permanently.

WHO DO I CONTACT? Contact ALL three to place the freeze.
Equifax • (800) 685-1111 or equifax.com/personal/credit-report-services
Experian • (888) 397-3742 or experian.com/help
TransUnion • (800) 680-7289 or transunion.com/credit-help

4 CONSIDER MAKING AN IDENTITY THEFT REPORT

4 CONSIDER MAKING AN IDENTITY THEFT REPORT

WHAT IS IT? An Identity Theft Report is made up of an affidavit from the Federal Trade Commission (FTC) and a police report. Together these items help you to dispute any accounts the identity thief opened using your information. See pages 3-4 for information on the value of an Identity Theft Report.

HOW DO I MAKE ONE? Contact the FTC to complete an Identity Theft Affidavit. Then, print out a copy of the affidavit for use in your Identity Theft Report. Take the affidavit with you to the police station to file your police report. If the officer is hesitant to give you a report, tell them you need an "information only" report. Attach your Identity Theft Affidavit to the police report.

WHO DO I CONTACT? Call the FTC (877) 438-4338 or visit IdentityTheft.gov.

REPAIR THE DAMAGE

There are different options for repairing the damage caused by identity theft. Choose the path that is right for you.

1 REVIEW YOUR CREDIT REPORTS

Go through each section with a fine tooth comb. Look for items you don't recognize. This could be anything from a misspelled name, an address where you've never lived, an account you didn't open or a judgment or lien you weren't aware of. Be sure to check your credit reports regularly.

2 CLOSE AFFECTED/FRAUDULENT ACCOUNTS

Contact the security or fraud department of each company. If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, request the forms needed to dispute those transactions. Send the forms certified mail, return receipt requested and keep a copy for your records.

3 CORRECTING ERRORS

If you find mistakes resulting from identity theft on your credit reports, you can dispute or block the information, but depends on if you've created an ID theft report. Head to page 3 for your next step.

CORRECTING ERRORS

If you find mistakes resulting from identity theft on your credit reports, you can dispute or block the information. Blocking requires an Identity Theft Report. See page 2 for the steps to make a report.

What is Disputing?

Federal law allows you to dispute inaccuracies on your credit report. To do this, contact the credit reporting agencies and the business that provided the inaccurate information. You can dispute inaccuracies whether they are the result of identity theft or not. **You will not need an Identity Theft Report to dispute information.**

***REMEMBER:** Send all letters **certified mail with return receipt requested.**

I DON'T have an Identity Theft Report



Disputing Fraudulent Accounts

With Credit Reporting Agencies:

- Write to the credit reporting agency explaining that you are a victim of identity theft.
- List any errors found on your credit report and include **copies** of supporting documents.

With Businesses:

- Request dispute forms from the business. Fill them out, detailing what information is inaccurate.
- In some cases, you can send a letter outlining what is incorrect.
- Send **copies** of any supporting documents along with your completed form/letter.

DID YOU KNOW? You can dispute online, too!

www.transunion.com
(click on Credit Help)

www.equifax.com
(click on Credit Report Assistance)

www.experian.com
(click on Credit Report Assistance)

What is Blocking?

By law, credit reporting agencies must block identity theft-related information from appearing on a victim's credit report. They must block unauthorized transactions, accounts, and inquiries. To get unauthorized information blocked, you must give certain information to the credit reporting agencies. **You will need an Identity Theft Report.**

I DO have an Identity Theft Report



Blocking Fraudulent Accounts

With Credit Reporting Agencies:

- Write to each credit reporting agency. Send a copy of your Identity Theft Report.
- Include proof of your identity: your name, address, and Social Security number.
- Explain which information on your report resulted from identity theft.
- Ask the agency to block the fraudulent information.

With Businesses:

- Write a letter to the business. Include a copy of your Identity Theft Report.
- Include proof of your identity, including your name, address, and Social Security number.
- Include a copy of your credit report. Explain which information on the credit report resulted from identity theft, and that it didn't come from a transaction you made or approved.

DAMAGE CONTROL

LONG TERM ALERTS

These **FREE** alerts can offer you even more protection than the initial fraud alert, but they have different conditions. So, read carefully and decide if either would apply to your situation.

Extended Fraud Alert

An extended fraud alert is only available to identity theft victims. The alert lasts for **seven years** and allows you to access **two copies** of your **credit report** from each credit reporting agency within a year of placing the alert. Your name will also be taken off marketing lists for prescreened credit offers for **five years**.

Unlike the initial fraud alert, you need to contact **EACH** credit reporting agency to get the extended fraud alert. The company may have you complete a request form and you *will* have to supply an Identity Theft Report.

The graphic below explains how to make an Identity Theft Report, which will help you prove you're a victim of identity theft. See page 2 for more information.



Active Duty Alert

This alert is available for military personnel who are deployed. To place the alert, contact **ONE** of the credit reporting agencies.



You may need to provide proof of identity, **such as a military ID, birth certificate or driver's license**. The alert will stay in place for **one year**, but can be renewed.

Your name will also be taken off marketing lists for prescreened credit offers for **two years**, unless you ask to be added back to the list.

HAS SOMEONE USED YOUR SOCIAL SECURITY NUMBER?



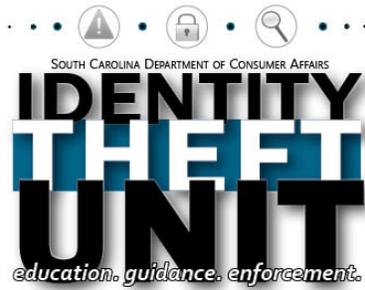
Someone illegally using your Social Security number (SSN) can cause a lot of problems. Identity thieves can use your info, like a SSN, the same way you do. Including to get:

- Government benefits
- Cell phones/utilities
- Tax Refund
- Driver's License/ID
- Medical benefits
- A Job

Make sure to sign up for my Social Security to monitor your account. This online tool (www.ssa.gov/myaccount) lets you view estimates of future retirement, manage benefits, change your address and direct deposit information, view earnings and Social Security and Medicare taxes you've paid and more. If someone is using your SSN for work, their earnings may show up on your statement. Once you create an account, it also prevents others from creating an account in your name. If you find any errors, contact the Social Security Administration (SSA). Find your local SSA Office by calling (866) 964-7594.

Security and Medicare taxes you've paid and more. If someone is using your SSN for work, their earnings may show up on your statement. Once you create an account, it also prevents others from creating an account in your name. If you find any errors, contact the Social Security Administration (SSA). Find your local SSA Office by calling (866) 964-7594.

SSN card lost or stolen? Visit www.ssa.gov/ssnumber for the steps to get a new card or call (866) 964-7594 to find your local SSA office.



© South Carolina Department of Consumer Affairs, 2021.
This brochure may be copied or reproduced for non-commercial,
educational purposes, so long as no changes or modifications are made.



PO Box 5757 • Columbia, SC 29250
(800) 922-1594 • www.consumer.sc.gov



Find the latest scam alerts and news here. twitter.com/scdca



Check out our YouTube channel. youtube.com/scdcatv



Look here for updates & educational materials. facebook.com/SCDepartmentofConsumerAffairs