

TAKING CHARGE



WHAT TO DO IF YOUR IDENTITY IS STOLEN



TAKING CHARGE

WHAT TO DO IF YOUR IDENTITY IS STOLEN

INTRODUCTION	3
IMMEDIATE STEPS	5
Place an Initial Fraud Alert	6
Order Your Credit Reports	8
Create an Identity Theft Report	9
NEXT STEPS	13
Review Your Credit Reports	13
Dispute Errors with Credit Reporting Companies	13
Blocking: Report Errors to the Credit Reporting Companies	17
Blocking: Report Errors to Businesses	18
Get Copies of Documents the Identity Thief Used	19
ATM and Debit Cards	20
Checking Accounts	21
Credit Cards	23
Bankruptcy Filed in Your Name	24
Investment Accounts	24

Debt Collectors	25
Government-Issued Identification	26
Mail Theft	27
Utilities	27
Student Loans	28
Misuse of Social Security Number	28
Income Taxes	29
Medical Identity Theft	30
Child Identity Theft	32
Criminal Violations	34
REDUCE YOUR RISK	37
Review Your Credit Reports	37
Review Your Explanation of Medical Benefits	38
Respond Quickly to Notices from the Internal Revenue Service	38
Active Duty Alerts for Military Personnel	39
Protect Your Personal Information	40
SAMPLE LETTERS AND FORMS	43

Contact info is provided on the inside back cover.

INTRODUCTION

Identity theft happens when someone steals your personal information and uses it without your permission. It is a serious crime that can wreak havoc with your finances, credit history, and reputation – and it can take time, money, and patience to resolve. The Federal Trade Commission (FTC), the nation’s consumer protection agency, prepared this guide to help you repair the damage that identity theft can cause, and reduce the risk of identity theft happening to you.

If you suspect that someone has stolen your identity, acting quickly is the best way to limit the damage. Setting things straight involves some work. This guide has tips, worksheets, blank forms, and sample letters to guide you through the recovery process. It covers:

- what identity theft victims must do immediately
- what problems may crop up
- how you can reduce your risk of identity theft

How do thieves get my information?

“I thought I kept my personal information to myself.”

You may have, but identity thieves are resourceful and use a variety of ways to get your information. They “dumpster dive” or rummage through your garbage, the trash of businesses, or public dumps. They may work – or pretend to work – for legitimate companies, medical offices, clinics, pharmacies, or government agencies, and take advantage of that role to convince you to reveal personal information. Some thieves pretend to represent an institution you trust, and try to trick you by email (phishing) or phone (pretexting) into revealing personal information.

What do identity thieves do with my information?

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief might even file a tax return in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

How can I tell that someone has stolen my information?

- you see unexplained withdrawals from your bank account
- you don't get your bills or other mail
- merchants refuse your checks
- debt collectors call you about debts that aren't yours
- you find unfamiliar accounts or charges on your credit report
- medical providers bill you for services you didn't use
- your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit
- the Internal Revenue Service (IRS) notifies you that more than 1 tax return was filed in your name, or that you have income from an employer you don't work for
- you get notice that your information was compromised by a data breach at a company where you do business or have an account
- you are arrested for a crime someone else allegedly committed in your name

What should I do if my information is lost or stolen, but my accounts don't show any problems?

If your wallet, Social Security card, or other personal, financial, or account information is lost or stolen, contact the credit reporting companies and place a fraud alert on your credit file. See how to place a fraud alert on page 6. Check your bank and other account statements for unusual activity. You may want to take additional steps, depending on what information was lost or stolen. For example, you can exercise your legal right to a free copy of your credit report.

If your information is lost in a data breach, the organization that lost your information will notify you and tell you about your rights. Generally, you may choose to:

- place a fraud alert on your credit file
- monitor your accounts for unusual activity
- exercise your right to a free copy of your credit report

You may have other rights under state law.





IMMEDIATE STEPS

This section explains the first steps to take if your identity is stolen:

- 1 Place an Initial Fraud Alert
- 2 Order Your Credit Reports
- 3 Create an Identity Theft Report

MONITOR YOUR PROGRESS

As you get started, create a system to organize your papers and track deadlines.

ITEM	HOW TO TRACK	TIPS
 Telephone Calls	Create a log of all telephone calls.	<ul style="list-style-type: none">• Record the date of each call and the names and telephone numbers of everyone you contact.• Prepare your questions before you call. Write down the answers.
 Postal Mail	Send letters by certified mail. Ask for a return receipt.	<ul style="list-style-type: none">• See sample letters starting at page 43.
 Documents	Create a filing system.	<ul style="list-style-type: none">• Keep all originals.• Send copies of your documents and reports, not originals. Make copies of your identification to include in letters.
 Deadlines	Make a timeline.	List important dates, including when: <ul style="list-style-type: none">• You must file requests• A company must respond to you• You must send follow-up

1 Place an Initial Fraud Alert

Three nationwide credit reporting companies keep records of your credit history. If you think someone has misused your personal or financial information, call 1 of the companies and ask them to put an initial fraud alert on your credit report. You must provide proof of your identity. The company you call must tell the other companies about your alert.

An initial fraud alert can make it harder for an identity thief to open more accounts in your name. When you have an alert on your report, a business must verify your identity before it issues credit in your name, so it may try to contact you. Be sure the credit reporting companies have your current contact information so they can get in touch with you. The initial alert stays on your report for 90 days. It allows you to order 1 free copy of your credit report from each of the 3 credit reporting companies.

HOW TO PLACE A FRAUD ALERT

STEP BY STEP:	NOTES:			
<input type="checkbox"/> Contact 1 credit reporting company.	<table border="1" data-bbox="581 842 1511 919"> <tr> <td data-bbox="581 842 857 919">Equifax 1-800-525-6285</td> <td data-bbox="857 842 1170 919">Experian 1-888-397-3742</td> <td data-bbox="1170 842 1511 919">TransUnion 1-800-680-7289</td> </tr> </table> <ul style="list-style-type: none"> <input type="checkbox"/> Report that you are an identity theft victim. <input type="checkbox"/> Ask the company to put a fraud alert on your credit file. <input type="checkbox"/> Confirm that the company you call will contact the other 2 companies. <p><i>Placing a fraud alert is free. The initial fraud alert stays on your credit report for 90 days.</i></p> <p><i>Be sure the credit reporting companies have your current contact information so they can get in touch with you.</i></p>	Equifax 1-800-525-6285	Experian 1-888-397-3742	TransUnion 1-800-680-7289
Equifax 1-800-525-6285	Experian 1-888-397-3742	TransUnion 1-800-680-7289		
<input type="checkbox"/> Learn about your rights.	<p><i>The credit reporting company will explain that you can get a free credit report, and other rights you have.</i></p>			
<input type="checkbox"/> Mark your calendar.	<p><i>The initial fraud alert stays on your report for 90 days. You can renew it after 90 days.</i></p>			
<input type="checkbox"/> Update your files.	<ul style="list-style-type: none"> <input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files. 			

Consider Requesting a Credit Freeze

You may want to contact the credit reporting companies to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely an identity thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. In many states, identity theft victims can place a freeze for free, but in others, victims must pay a fee, which is usually about \$10. If you have a police report, you may be able to place or lift a freeze for free.

Putting a credit freeze on your credit file does not affect your credit score. If you place a credit freeze on your credit file, you can:

- get a copy of your free annual credit report
- open a new account, apply for a job, rent an apartment, buy insurance, refinance your mortgage, or do anything else that requires your credit report

If you want a business, lender, or employer to be able to review your credit report, you must ask the credit reporting company to lift the freeze. You can ask to lift the freeze temporarily or permanently. You may be charged a fee to lift the freeze.

HOW TO REQUEST A CREDIT FREEZE

STEP BY STEP:	NOTES:			
<input type="checkbox"/> Contact your state Attorney General's office.	<p><i>Find your state Attorney General's office at www.naag.org to determine what your state allows.</i></p> <input type="checkbox"/> Ask if there is a fee for putting a freeze on your credit file. <input type="checkbox"/> Ask how long the freeze lasts.			
<input type="checkbox"/> Contact each credit reporting company.	<table border="0" style="width: 100%;"> <tr> <td style="text-align: center; vertical-align: top;"><i>Equifax</i> 1-800-525-6285</td> <td style="text-align: center; vertical-align: top;"><i>Experian</i> 1-888-397-3742</td> <td style="text-align: center; vertical-align: top;"><i>TransUnion</i> 1-800-680-7289</td> </tr> </table> <input type="checkbox"/> Report that you are an identity theft victim. <input type="checkbox"/> Ask the company to put a freeze on your credit file. <input type="checkbox"/> Pay the fee required by state law.	<i>Equifax</i> 1-800-525-6285	<i>Experian</i> 1-888-397-3742	<i>TransUnion</i> 1-800-680-7289
<i>Equifax</i> 1-800-525-6285	<i>Experian</i> 1-888-397-3742	<i>TransUnion</i> 1-800-680-7289		
<input type="checkbox"/> Mark your calendar.	<p><i>Your state law determines how long the credit freeze lasts.</i></p>			
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.			

2 Order Your Credit Reports

After you place an initial fraud alert, the credit reporting company will explain your rights and how you can get a copy of your credit report. **Placing an initial fraud alert entitles you to a free credit report from each of the 3 credit reporting companies.**

HOW TO ORDER YOUR FREE CREDIT REPORTS

STEP BY STEP:	NOTES:		
<input type="checkbox"/> Contact each credit reporting company.	Equifax 1-800-525-6285	Experian 1-888-397-3742	TransUnion 1-800-680-7289
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Explain that you placed an initial fraud alert. <input type="checkbox"/> Order your free copy of your credit report. <input type="checkbox"/> Ask each company to show only the last 4 digits of your Social Security number on your report. <input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.		

Contact Businesses

If you know which of your accounts have been tampered with, contact the related businesses. Talk to someone in the fraud department, and follow up in writing. Send your letters by certified mail; ask for a return receipt. That creates a record of your communications.

When you read your credit report, you may find unauthorized charges or accounts. Learn how to review your credit report and dispute errors on page 13.

3 Create an Identity Theft Report

An Identity Theft Report helps you deal with credit reporting companies, debt collectors, and businesses that opened accounts in your name. You can use the Report to:

- get fraudulent information removed from your credit report
- stop a company from collecting debts that result from identity theft, or from selling the debt to another company for collection
- place an extended fraud alert on your credit report
- get information from companies about accounts the identity thief opened or misused

Creating an Identity Theft Report Involves 3 Steps:

- 1 Submit a complaint about the theft to the FTC. When you finish writing all the details, print a copy of the report. It will print as an Identity Theft Affidavit.
- 2 File a police report about the identity theft, and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit when you file a police report.
- 3 Attach your FTC Identity Theft Affidavit to your police report to make an Identity Theft Report.

Some companies want more information than the Identity Theft Report includes, or want different information. The information you need to provide depends on the policies of the credit reporting company and the business that sent the information about you to the credit reporting company.



HOW TO REPORT IDENTITY THEFT TO THE FTC AND PRINT AN FTC IDENTITY THEFT AFFIDAVIT

ONLINE

STEP BY STEP:	NOTES:
<input type="checkbox"/> Complete the FTC's online complaint form.	<p>www.ftc.gov/complaint</p> <ul style="list-style-type: none"> <input type="checkbox"/> Complete the complaint form with as many details as you know. <input type="checkbox"/> Review the form and click "submit." <input type="checkbox"/> Save the complaint reference number that appears after you submit your information. <p><i>You'll need your complaint reference number to update your complaint online or by phone.</i></p>
<input type="checkbox"/> Save or print your FTC Identity Theft Affidavit.	<ul style="list-style-type: none"> <input type="checkbox"/> Click on the words "Click here to get your completed FTC Identity Theft Affidavit." <p><i>Before you leave that screen, be sure you saved or printed your Affidavit. You cannot save or print it after you leave this screen.</i></p>

OR

BY PHONE

STEP BY STEP:	NOTES:
<input type="checkbox"/> Call the FTC.	<p>1-877-438-4338 1-866-653-4261 (TTY)</p> <ul style="list-style-type: none"> <input type="checkbox"/> Tell the representative what happened. <input type="checkbox"/> Ask for your complaint reference number and Affidavit password. <p><i>The FTC representative will email you a link so you can get your Affidavit.</i></p>
<input type="checkbox"/> Save or print your FTC Identity Theft Affidavit.	<ul style="list-style-type: none"> <input type="checkbox"/> Go to the link the representative sent you. <input type="checkbox"/> Enter your complaint reference number, Affidavit password, and your email address. <input type="checkbox"/> Print or save your Identity Theft Affidavit.

THEN

STEP BY STEP:	NOTES:
<input type="checkbox"/> Update your files.	<ul style="list-style-type: none"> <input type="checkbox"/> Record the dates you filed your complaint. <input type="checkbox"/> Keep copies of your Affidavit in your files.
<input type="checkbox"/> If necessary, call the FTC to update your complaint.	<p>1-877-438-4338 1-866-653-4261 (TTY)</p> <p><i>Be ready to provide your complaint reference number.</i></p>

HOW TO FILE A POLICE REPORT

STEP BY STEP:	NOTES:
<input type="checkbox"/> Go to your local police department or the police department where the theft occurred.	<input type="checkbox"/> Bring a copy of your FTC Identity Theft Affidavit and any other proof of the theft. <input type="checkbox"/> Complete a report about the theft. <input type="checkbox"/> Ask to have a copy, or the number, of the report. <i>In some states, police must take your report. Visit www.naag.org to see what your state law requires.</i> <i>If the police won't take a report about the identity theft, ask if you can file a "miscellaneous incidents" report, or go to a different police station, or the sheriff's department, state police or federal authority.</i> <i>You can give police a copy of the FTC's Memo to Law Enforcement, which explains how Identity Theft Reports are important to victims. See the memo in the back of this book on page D-1.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or visits. <input type="checkbox"/> Record your police report number. <input type="checkbox"/> Keep a copy of your police report in your files.

HOW TO CREATE YOUR IDENTITY THEFT REPORT

STEP BY STEP:	NOTES:
<input type="checkbox"/> Attach your FTC Identity Theft Affidavit to your police report.	<input type="checkbox"/> Keep a complete copy in your files.

Consider Placing an Extended Fraud Alert

If you are a victim of identity theft and have created an Identity Theft Report, you can place an extended fraud alert on your credit file. It stays in effect for 7 years. When you place an extended alert:

- you can get 2 free credit reports within 12 months from each of the 3 nationwide credit reporting companies
- the credit reporting companies must take your name off marketing lists for prescreened credit offers for 5 years, unless you ask them to put your name back on the list

HOW TO PLACE AN EXTENDED FRAUD ALERT

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact each credit reporting company. <i>See contact info on inside back cover.</i>	<input type="checkbox"/> Ask the company to place an extended fraud alert on your credit file. <i>The company may have you complete a request form.</i> <input type="checkbox"/> Include a copy of your Identity Theft Report when you submit the form and your letter. <i>Placing an extended fraud alert is free.</i>
<input type="checkbox"/> Mark your calendar.	<i>The extended alert stays in effect for 7 years.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

NEXT STEPS

Review Your Credit Reports

If you know an identity thief tampered with some of your accounts, you may have contacted the related businesses already. After you get your credit reports, read them to see whether other fraudulent transactions or accounts are listed.

Your credit report is full of information about where you live, how you pay your bills, and whether you've been sued or arrested, or have filed for bankruptcy. The information in your credit report is used to evaluate your applications for credit, insurance, employment, and renting a home, so it's important that the information is accurate and up-to-date. Check all key information, including your:

- name
- address
- Social Security number
- employers

If you see errors on the report, like accounts you didn't open or debts you didn't incur, contact the credit reporting companies and the fraud department of each business that reported an error.

Dispute Errors with Credit Reporting Companies

If you find mistakes when you review your credit reports, send letters explaining the mistakes to:

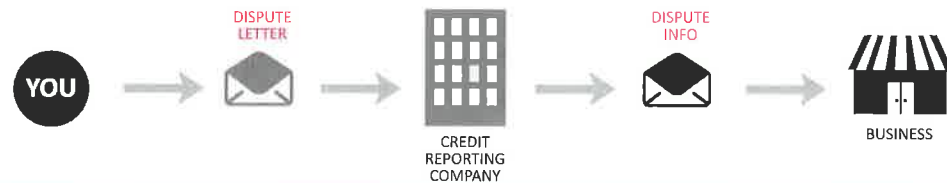
- the 3 nationwide credit reporting companies
- the fraud department of each business that reported a fraudulent transaction on your existing accounts
- the fraud department of each business that reported a new account opened in your name by an identity thief

If the errors result from identity theft and you have an Identity Theft Report, ask the credit reporting companies and business to block the disputed information from appearing on your credit reports. The credit reporting companies must block transactions and accounts if you are an identity theft victim. Read about blocking on page 17.

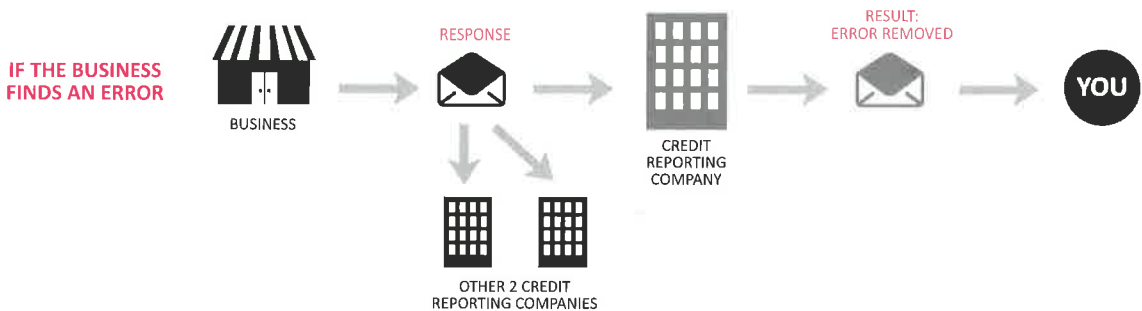
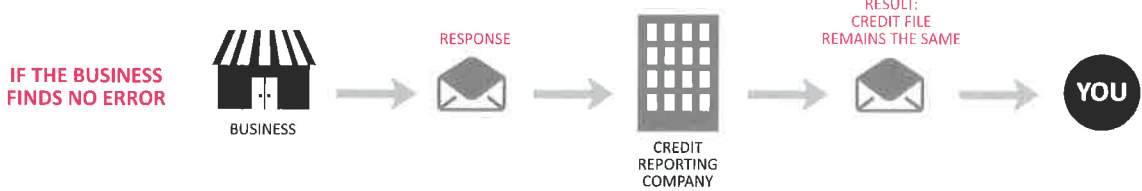
HOW TO DISPUTE ERRORS WITH CREDIT REPORTING COMPANIES

STEP BY STEP:	NOTES:
<input type="checkbox"/> Write to each credit reporting company. <i>See contact info on inside back cover.</i> <i>See sample letter on page C-1.</i>	<input type="checkbox"/> Explain that you are an identity theft victim. <input type="checkbox"/> List the errors that you found. <input type="checkbox"/> Include copies of documents showing the errors. <input type="checkbox"/> Ask the credit reporting company to remove fraudulent information. <i>The credit reporting company must investigate the items you send, and forward that information to the business that reported the information to the credit reporting company.</i>
<input type="checkbox"/> Receive response from each credit reporting company.	<i>If your credit file changes because of the business' investigation, the credit reporting company must send you a letter with the results.</i> <i>If the credit reporting company puts the information back in your file, it must send you a letter telling what it did.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

After the business gets notice from the credit reporting company, it has 30 days to investigate and respond to the credit reporting company. If the business finds an error, it must notify the credit reporting company so your credit file can be corrected. If your credit file changes because of the business' investigation, the credit reporting company must send you a letter with the results. The credit reporting company can't add the disputed information back into your file unless the business says the information is correct. If the credit reporting company puts the information back in your file, it must send you a letter telling you that.



THE BUSINESS HAS 30 DAYS TO INVESTIGATE



HOW TO DISPUTE FRAUDULENT CHARGES ON YOUR EXISTING ACCOUNTS

STEP BY STEP:	NOTES:
<input type="checkbox"/> Change the passwords or PINs for your accounts.	<p><i>See tips on creating a strong password on page 42.</i></p>
<input type="checkbox"/> Ask each business if it will accept your Identity Theft Report or if it uses special dispute forms.	<input type="checkbox"/> If you must use the business' forms, ask for blank forms.
<input type="checkbox"/> Write to the fraud department of each business.	<ul style="list-style-type: none"> <input type="checkbox"/> Use the address they specify for disputes. <input type="checkbox"/> Explain that you are an identity theft victim. <input type="checkbox"/> List the errors you found. <input type="checkbox"/> Send copies of documents that show the error. <input type="checkbox"/> Ask the business to remove fraudulent information. <input type="checkbox"/> Include a copy of your Identity Theft Report (or the special dispute forms if the business requires them). <input type="checkbox"/> Include a copy of your credit report. Black out any personal information that does not pertain to your dispute. <p><i>See sample letter at the back of this book on page A-1.</i></p> <p><i>The business must review your letter, investigate your complaint, and tell you the results of their investigation. If the information is wrong, the business must tell the credit reporting company.</i></p>
<input type="checkbox"/> Ask the business to send you a letter confirming that it removed the fraudulent information.	<input type="checkbox"/> Keep the letter in case you see fraudulent information on your statement later.
<input type="checkbox"/> Update your files.	<ul style="list-style-type: none"> <input type="checkbox"/> Record the dates that you changed passwords and PINs. <input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

HOW TO DISPUTE FRAUDULENT ACCOUNTS OPENED IN YOUR NAME

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the fraud department of each business where an account was opened.	<input type="checkbox"/> Explain that you are an identity theft victim. <input type="checkbox"/> Close the account. <input type="checkbox"/> Ask if the business will accept your Identity Theft Report or if it uses special dispute forms. If you must use the business' forms, ask for blank forms.
<input type="checkbox"/> Send a copy of your Identity Theft Report or the business' dispute forms.	<i>See sample letter at the back of this book on page B-1.</i> <input type="checkbox"/> Ask the business to send you a letter confirming that: <ul style="list-style-type: none">• the fraudulent account isn't yours• you aren't liable for it• it was removed from your credit report <input type="checkbox"/> Keep the letter and use it if you see this account on your credit report in the future.
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Blocking: Report Errors to the Credit Reporting Companies

By law, credit reporting companies 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 information to the credit reporting companies.

HOW TO ASK CREDIT REPORTING COMPANIES TO BLOCK INFORMATION

STEP BY STEP:	NOTES:
<input type="checkbox"/> Write to each credit reporting company. <i>See contact info on inside back cover.</i>	<input type="checkbox"/> Send a copy of your Identity Theft Report. <input type="checkbox"/> Include proof of your identity including your name, address, and Social Security number. <input type="checkbox"/> Explain which information on your report resulted from identity theft and that the information didn't come from a transaction you made or approved. <input type="checkbox"/> Ask the company to block the fraudulent information. <i>You can get sample letters at www.ftc.gov/idtheft.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

If the credit reporting company accepts your Identity Theft Report, it must block the fraudulent information from your credit report within 4 business days after accepting your Report, and tell the business that sent the fraudulent information about the block.

If the credit reporting company rejects your Identity Theft Report, it can take 5 days to ask you for more proof of the identity theft. It has 15 more days to work with you to get the information, and 5 days to review information you sent. It may reject any information you send after 15 days. It must tell you if it won't block information. You can re-submit the Report.

After a business has been notified about a block of fraudulent information, it must:

- stop reporting that information to all the credit reporting companies.
- not sell or transfer a debt for collection.

Blocking: Report Errors to Businesses

Contact the business that sent the inaccurate information that appears on your credit report. Send a copy of your Identity Theft Report and a letter explaining what is inaccurate. After the business gets your Report, it must stop reporting the inaccurate information to the 3 nationwide credit reporting companies. However, the business still can try to collect a debt, and sell or transfer the debt to a collection company.

To prevent a business from collecting, selling or transferring a debt to a collection agency, you must contact the credit reporting companies and ask them to block fraudulent information. To do this, follow the steps on page 17, How to Ask Credit Reporting Companies to Block Information.

HOW TO ASK A BUSINESS TO BLOCK INFORMATION

STEP BY STEP:	NOTES:
<input type="checkbox"/> Write to the business that has records of the fraudulent transactions.	<input type="checkbox"/> Include a copy of your Identity Theft Report. <input type="checkbox"/> Include proof of your identity, including your name, address, and Social Security number. <input type="checkbox"/> Include a copy of your credit report. <input type="checkbox"/> Explain which information on the credit report resulted from identity theft, and that it didn't come from a transaction you made or approved. <i>The business must stop reporting the inaccurate information to the 3 nationwide credit reporting companies. The business can continue to try to collect the debt, and sell or transfer the debt to a collection company.</i> <i>To prevent a business from collecting, selling or transferring a debt, follow the steps on page 17.</i> <i>You can get sample letters at www.ftc.gov/idtheft.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Get Copies of Documents the Identity Thief Used

Ask for copies of any documents the identity thief used to open a new account or make charges in your name. These documents can help prove the identity theft.

HOW TO GET COPIES OF DOCUMENTS THE IDENTITY THIEF USED

STEP BY STEP:	NOTES:
<p><input type="checkbox"/> Contact the business that has records of transactions the identity thief made.</p> <p>OR</p> <p><input type="checkbox"/> Give written permission to a law enforcement officer to contact the company on your behalf.</p>	<p><input type="checkbox"/> Ask for copies of documents the thief used to open new accounts or charge purchases in your name.</p> <p><input type="checkbox"/> Send details about where or when the fraudulent transactions took place.</p> <p><input type="checkbox"/> Include a copy of your Identity Theft Report or the proof the business requires, and proof of your identity.</p> <p><i>The business must send you free copies of the records within 30 days of getting your request. For example, if you dispute a debt on a credit card account you did not open, ask for a copy of the application and applicant's signature.</i></p> <p><i>You can get sample letters at www.ftc.gov/idtheft.</i></p>
<p><input type="checkbox"/> Update your files.</p>	<p><input type="checkbox"/> Record the dates you made calls or sent letters.</p> <p><input type="checkbox"/> Keep copies of letters in your files.</p>

ATM and Debit Cards

As an identity theft victim, you have protections under federal law for ATM or debit card transactions. Federal law also limits your liability for the unauthorized electronic transfer of funds that result from identity theft.

It's best to act as soon as you discover a withdrawal or purchase you didn't make or authorize. Many card issuers have voluntarily agreed that an account holder will not owe more than \$50 for transactions made with a lost or stolen ATM or debit card. However, under the law, the amount you can lose depends on **how quickly** you report the loss. If you don't report within 60 days of the day your institution sent you the account statement showing the unauthorized withdrawals, you could lose all the money an identity thief took from your account.

HOW TO REPORT FRAUDULENT TRANSACTIONS

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact your ATM or debit card issuer.	<input type="checkbox"/> Report the fraudulent transaction. <i>Act as soon as you discover a withdrawal or purchase you didn't make.</i>
<input type="checkbox"/> Write a follow up letter to confirm that you reported the problem.	<input type="checkbox"/> Keep a copy of your letter. <input type="checkbox"/> Send it by certified mail and ask for a return receipt.
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Limit Your Loss

HOW QUICKLY YOU REPORT THE PROBLEM <i>after your card issuer sends you the statement showing unauthorized purchases or withdrawals</i>	YOUR MAXIMUM LOSS
Within 2 business days	\$50
2-60 business days later	\$500
More than 60 business days later	All the money taken from your ATM/debit card

In most cases, the financial institution has 10 business days to investigate your report of a fraudulent transaction. It must tell you the results within 3 days of finishing the investigation and fix an error within 1 business day of finding it. In some cases, it can take 45 days to finish the investigation.

Checking Accounts

An identity thief may steal your paper checks, misuse the account number from the bottom of your checks, or open a new account in your name. If this happens, contact your bank or financial institution and ask them to close the account as soon as possible.

Federal law doesn't limit your loss if a thief forges your signature on your checks or uses your account number to buy something by phone, but most states hold banks responsible for losses from those fraudulent transactions. However, banks expect their customers to take reasonable care of their accounts. That means you might be responsible for a loss if you know about a problem but don't report it to your bank quickly.

HOW TO REPORT STOLEN CHECKS

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact your financial institution.	<input type="checkbox"/> Ask it to stop payment on stolen checks and close your account. <input type="checkbox"/> Ask it to report the theft to its check verification system. <i>The check verification system will tell businesses to refuse the stolen checks.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

OR

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact check verification companies.	<input type="checkbox"/> Report that your checks were stolen. <input type="checkbox"/> Ask them to tell businesses to refuse the stolen checks. <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> TeleCheck 1-800-710-9898 </div> <div style="text-align: center;"> Certegy, Inc. 1-800-437-5120 </div> </div>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

HOW TO REPORT CHECKING ACCOUNTS OPENED IN YOUR NAME

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact ChexSystems, Inc., to request a free ChexSystems report.	<input type="checkbox"/> Order a free copy of the ChexSystems report that lists checking accounts opened in your name. ChexSystems, Inc. www.consumerdebit.com 1-800-428-9623
<input type="checkbox"/> Contact every financial institution where a new account was opened.	<input type="checkbox"/> Ask the financial institution to close the account.
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

WHAT IF A BUSINESS REJECTS YOUR CHECK?

STEP BY STEP:	NOTES:
<input type="checkbox"/> Ask the business for an explanation.	<i>The business must tell you what information it used to decide to reject the check.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

WHAT IF A THIEF PASSES BAD CHECKS IN YOUR NAME?

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the business that took the bad check.	<input type="checkbox"/> Explain that you are a victim of identity theft before they start collection action against you.
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Get Help from Bank or Financial Institution Regulators

If you are working with a bank or financial institution to resolve identity theft-related problems and need help, contact the agency that oversees the bank or financial institution.

Visit www.ffiec.gov/consumercenter to find out which agency to contact.

Credit Cards

Your liability for credit card charges that you didn't authorize is limited to \$50 per card. To dispute fraudulent charges, contact the credit card issuer within 60 days of the day the credit card issuer sends you the bill showing the fraudulent charges.

What if an identity thief changed the address on your account and you don't get your statement? You are responsible for keeping track of your statements. If your statement doesn't arrive on time, contact your credit card company.

HOW TO DISPUTE FRAUDULENT CHARGES ON YOUR CREDIT CARD

STEP BY STEP:

NOTES:

Write to your credit card issuer.

- Write within 60 days of the day the credit card issuer sent you the bill showing the fraudulent charges.
- Write to the address specified for billing inquiries, not the payment address.
- Identify the amount and date of the billing error.
- Include your name, address, account number, and a copy of your Identity Theft Report or other proof of identity theft.
- Send the letter by certified mail and ask for a return receipt.

See sample letter at the back of this book on page A-1.

Within 30 days of getting your complaint, the credit card company must send you a letter acknowledging it, unless your complaint has been resolved. The company must resolve the dispute within 2 billing cycles, or in less than 90 days after getting your complaint.

Update your files.

- Record the dates you made calls or sent letters.
- Keep copies of letters in your files.

Bankruptcy Filed in Your Name

If you believe someone filed for bankruptcy in your name, contact the U.S. Trustee in the region where the bankruptcy was filed. The U.S. Trustee Program refers cases of suspected bankruptcy fraud to the United States Attorneys for possible investigation and prosecution. The U.S. Trustee can't provide you with legal help, so you may need to hire an attorney.

HOW TO REPORT BANKRUPTCY FILED IN YOUR NAME

STEP BY STEP:	NOTES:
<input type="checkbox"/> Write to the U.S. Trustee in the region where the bankruptcy was filed.	<input type="checkbox"/> Find regional offices at www.usdoj.gov/ust or in the Blue Pages of the phone book under U.S. Government Bankruptcy Administration. <input type="checkbox"/> Describe the situation and provide proof of your identity.
<input type="checkbox"/> Consider hiring an attorney.	<i>An attorney can explain to the court that the bankruptcy filing was fraudulent.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Investment Accounts

If an identity thief has tampered with your investments or brokerage accounts, contact your broker, account manager, and the U.S. Securities and Exchange Commission (SEC).

HOW TO DEAL WITH AFFECTED INVESTMENT ACCOUNTS

STEP BY STEP:	NOTES:
<input type="checkbox"/> Call your broker or account manager.	<input type="checkbox"/> Describe the situation.
<input type="checkbox"/> File a complaint with the SEC.	www.sec.gov/complaint.shtml or write to: <i>SEC Office of Investor Education and Advocacy 100 F Street, NE Washington, DC 20549</i>
<input type="checkbox"/> Call the SEC for general information.	<i>1-800-732-0330</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Debt Collectors

A debt collector may contact you if an identity thief opens accounts in your name but doesn't pay the bills. To stop contact and collection action, contact the debt collector, the business that opened the fraudulent account, and the credit reporting companies.

HOW TO DISPUTE A DEBT WITH A DEBT COLLECTOR

STEP BY STEP:	NOTES:
<input type="checkbox"/> Write to the debt collector within 30 days after you get written notice of the debt.	<input type="checkbox"/> Tell the debt collector you are a victim of identity theft and don't owe the debt. <input type="checkbox"/> Send copies of your police report, Identity Theft Report, or other documents that detail the identity theft. <i>The collector must suspend collection efforts until it sends you written verification of the debt. If the collector works for another company, it must tell the other company you are an identity theft victim.</i> <i>See How to Permanently Stop Calls and Letters from a Debt Collector on page 26.</i>
<input type="checkbox"/> Contact the business where the fraudulent account was opened.	<input type="checkbox"/> Explain that this is not your debt. <input type="checkbox"/> Ask for information about the transactions that created the debt. <i>The business must give you details about the transaction if you ask. For example, if you dispute a debt on a credit card account you did not open, ask for a copy of the application and applicant's signature.</i>
<input type="checkbox"/> Contact the 3 nationwide credit reporting companies.	<input type="checkbox"/> Take steps to have fraudulent information blocked from your credit report and to stop a business from selling or transferring a debt for collection. <i>Follow the steps on page 17, How to Ask Credit Reporting Companies to Block Information.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

HOW TO STOP A DEBT COLLECTOR FROM SELLING OR TRANSFERRING A DEBT

Follow the steps on page 17, How to Ask Credit Reporting Companies to Block Information.

After each credit reporting company accepts your Identity Theft Report, it must tell the debt collector that the debt may be caused by identity theft. Then, the debt collector can't sell or transfer the debt or report it to a credit reporting company.

HOW TO PERMANENTLY STOP CALLS AND LETTERS FROM A DEBT COLLECTOR

STEP BY STEP:	NOTES:
<input type="checkbox"/> Write a letter to the debt collector.	<input type="checkbox"/> Tell them to stop contacting you about the debt. <i>After the debt collector gets the letter, it can't contact you again, except once – to say it won't contact you again, or that it plans to take specific action. Sending this letter should stop calls and letters from the collector, but it doesn't prevent the debt collector from suing you to collect the debt.</i> <i>To stop collection action, follow the steps on page 17.</i> <i>You can get sample letters at www.ftc.gov/idtheft.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Government-Issued Identification

If your government-issued identification – for example your driver's license, passport, or Medicare card – has been lost, stolen, or fraudulently misused, contact the agency that issued the identification.

HOW TO REPORT A LOST, STOLEN OR MISSING DRIVER'S LICENSE

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the Department of Motor Vehicles in your state.	<input type="checkbox"/> Cancel the lost or stolen item and get a replacement. <input type="checkbox"/> Ask the agency to put a note in your file so no one else can get a license or ID in your name.
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

HOW TO REPORT A LOST, STOLEN OR MISSING PASSPORT

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the U.S. Department of State.	www.travel.state.gov/passport OR <i>Find a local Department of State office online or in the Blue Pages of the phone book.</i>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Mail Theft

Sometimes an identity thief steals mail and uses it to get your personal and financial information, open new accounts, or commit tax fraud. The U.S. Postal Inspection Service, which investigates cases of identity theft, wants you to contact them and make a report.

HOW TO REPORT MAIL THEFT

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the U.S. Postal Inspection Service office near your home.	<p><i>Find the nearest office at https://postalinspectors.uspis.gov</i></p> <p>OR</p> <p><i>Go to your local post office to find the address.</i></p>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Utilities

An identity thief may use your personal and financial information to get telephone, cable, electric, water, or other services. Report fraudulent accounts to the service provider as soon as you discover them.

HOW TO REPORT FRAUDULENT UTILITY CHARGES AND ACCOUNTS

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the utility or service provider.	<input type="checkbox"/> Close the account that the identity thief opened.
<input type="checkbox"/> Contact your state Public Utility Commission for additional help.	<p><i>Search online at www.naruc.org/commissions or check the Blue Pages of your phone book.</i></p>
<input type="checkbox"/> Contact the Federal Communications Commission for help with cell phone or telephone services.	<p><i>1-888-225-5322 1-888-835-5322 (TTY)</i></p> <p><i>Consumer & Governmental Affairs Bureau 445 12th Street, SW Washington, DC 20554 www.fcc.gov/cgb</i></p>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Student Loans

An identity thief may use your personal or financial information to get a student loan. Contact the school or program that opened the loan and ask them to close the loan.

HOW TO REPORT FRAUDULENT STUDENT LOANS

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the U.S. Department of Education.	<p>www.ed.gov/about/offices/list/oig/hotline.html 1-800-647-8733 U.S. Department of Education Office of the Inspector General 400 Maryland Avenue, SW Washington, DC 20202</p>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Misuse of Social Security Number

An identity thief may steal your Social Security number and sell it, or use the number to get a job or other benefits. Contact the Social Security Administration when you discover any misuse of your Social Security number.

HOW TO REPORT MISUSE OF YOUR SOCIAL SECURITY NUMBER

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the Social Security Administration.	<p>www.socialsecurity.gov Fraud Hotline 1-800-269-0271 1-866-501-2101 (TTY) Social Security Administration Fraud Hotline P.O. Box 17785 Baltimore, MD 21235</p>
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

Income Taxes

If someone uses your Social Security number to get a job, the employer will report the person's earnings to the Internal Revenue Service (IRS). When you file your tax return, you won't include those earnings. But, IRS records will show you failed to report all your income, and you can expect to get a letter from the IRS.

If someone uses your Social Security number and files a tax return in your name before you file, they may get your refund. When you file your own return later, IRS records will show the first filing and refund, and you'll get a letter from the IRS.

If you think someone has misused your Social Security number to get a job or tax refund – or the IRS sends you a notice indicating a problem – contact the IRS immediately. Specialists will work with you to protect your account.

HOW TO REPORT INCOME TAX FRAUD

STEP BY STEP:

NOTES:

Contact the Internal Revenue Service.

IRS Identity Protection Specialized Unit
1-800-908-4490
www.irs.gov/identitytheft

- Report the fraud and ask for the IRS ID Theft Affidavit Form 14039.
- Send a copy of your police report or an IRS Identity Theft Affidavit Form 14039 and proof of your identity, such as a copy of your Social Security card, driver's license or passport.

Update your files.

- Record the dates you made calls or sent letters.
- Keep copies of letters in your files.

Medical Identity Theft

If an identity thief gets medical treatment using your name, the thief's medical information – for example, blood type, test results, allergies, or illnesses – can get into your medical file. Information about the thief can be added to your medical, health insurance, and payment records.

If you suspect an identity thief has used your medical information, get copies of your medical records. Under federal law, you have a right to know what's in your medical files. Contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and anywhere you believe the thief has used your information. For example, if a thief got a prescription in your name, ask for the record from the pharmacy that filled the prescription and the health care provider who wrote the prescription. You may need to pay a fee to get copies of your records.

A provider might refuse to give you copies of your medical or billing records because it thinks that would violate the identity thief's privacy rights. A provider who thinks that is mistaken: you have the right to know what's in your file. If a provider denies your request, you have a right to appeal. Contact the person the provider lists in its Notice of Privacy Practices, the patient representative, or the ombudsman. Explain the situation and ask for your file. If the provider refuses to provide your records within 30 days of your written request, you may complain to the U.S. Department of Health and Human Services' Office for Civil Rights at www.hhs.gov/ocr.

The medical provider or office that created the information must change any inaccurate or incomplete information in your files. They also should tell labs, other health care providers, and anyone else that might have gotten incorrect information. If an investigation doesn't resolve your dispute, ask that a statement of the dispute be included in your record.

If a debt collector contacts you about a medical bill incurred by an identity thief, read more about dealing with debt collectors on page 25.

HOW TO CORRECT ERRORS IN YOUR MEDICAL RECORDS

STEP BY STEP:

NOTES:

<p><input type="checkbox"/> Contact each health care provider and ask for copies of your medical records.</p>	<p><input type="checkbox"/> Check your state's health privacy laws. Some state laws make it easier to get copies of your medical records.</p> <p><i>Visit www.hpi.georgetown.edu/privacy/records.html to review your state law rights.</i></p> <p><input type="checkbox"/> Complete the request form and pay any fees required to get copies of your records.</p> <p><i>If your provider refuses to give you copies of your records because it thinks that would violate the identity thief's privacy rights, you can appeal. Contact the person the provider lists in its Notice of Privacy Practices, the patient representative, or the ombudsman. Explain the situation and ask for your file.</i></p> <p><i>If the provider refuses to provide your records within 30 days of your written request, you may complain to the U.S. Department of Health and Human Services Office for Civil Rights at www.hhs.gov/ocr.</i></p>
<p><input type="checkbox"/> Review your medical records and report any errors to your health care provider.</p>	<p><input type="checkbox"/> Write to your health care provider to report mistakes in your medical records.</p> <p><input type="checkbox"/> Include a copy of the medical record showing the mistake.</p> <p><input type="checkbox"/> Explain why this is a mistake and how to correct it.</p> <p><input type="checkbox"/> Include a copy of your police report or Identity Theft Report.</p> <p><input type="checkbox"/> Send the letter by certified mail and ask for a return receipt.</p> <p><i>Your health care provider should respond to your letter within 30 days. It must fix the mistake and notify other health care providers who may have the same mistake in their records.</i></p>
<p><input type="checkbox"/> Notify your health insurer and all 3 credit reporting companies.</p>	<p><input type="checkbox"/> Send copies of your police report or Identity Theft Report to your health insurer's fraud department and the 3 nationwide credit reporting companies.</p> <p><i>See contact info on inside back cover.</i></p>
<p><input type="checkbox"/> Order copies of your credit reports if you haven't already.</p>	<p><i>See page 8. Check to see if there are debts caused by an identity thief.</i></p>
<p><input type="checkbox"/> Consider placing a fraud alert or security freeze on your credit files.</p>	<p><i>See page 6.</i></p>
<p><input type="checkbox"/> Update your files.</p>	<p><input type="checkbox"/> Record the dates you made calls or sent letters.</p> <p><input type="checkbox"/> Keep copies of letters in your files.</p>

Criminal Violations

If an identity thief uses your name, date of birth, Social Security number, or other personal information during an investigation or arrest, the information will be added to your state's criminal database. The information also may be added to a national criminal database.

If you learn who the thief is, ask the criminal records database manager(s) to change the "key name" in the database. That way, the records will show the thief's name instead of yours. Contact the agency that made the arrest, the court that convicted the identity thief, and your state Attorney General's office to get documents that will help you show your innocence.

HOW TO CLEAR YOUR NAME OF CRIMINAL CHARGES

STEP BY STEP:	NOTES:
<input type="checkbox"/> Contact the law enforcement agency that arrested the thief.	<input type="checkbox"/> File a report about the impersonation. <input type="checkbox"/> Give copies of your fingerprints, photograph, and identifying documents. <input type="checkbox"/> Ask the law enforcement agency to: <ul style="list-style-type: none">• compare your information to the imposter's• change all records from your name to the imposter's name• give you a "clearance letter" or "certificate of release" to declare your innocence
<input type="checkbox"/> Keep the clearance letter or "certificate of release" with you at all times.	
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

WHAT TO DO IF A COURT PROSECUTED A CASE AGAINST A THIEF WHO USED YOUR NAME

STEP BY STEP:

NOTES:

<input type="checkbox"/> Contact the court where the arrest or conviction happened.	<input type="checkbox"/> Ask the district attorney for records to help you clear your name in court records. <input type="checkbox"/> Provide proof of your identity. <input type="checkbox"/> Ask the court for a "certificate of clearance" that declares you are innocent.
<input type="checkbox"/> Keep the "certificate of clearance" with you at all times.	
<input type="checkbox"/> Contact your state Attorney General.	<i>Find your state Attorney General's office at www.naag.org.</i> <input type="checkbox"/> Ask if your state has an "identity theft passport" or some kind of special help for identity theft victims.
<input type="checkbox"/> If you obtain an identity theft passport, keep it with you at all times.	
<input type="checkbox"/> Consider hiring a criminal defense lawyer.	<i>Your state Bar Association or Legal Services provider can help you find a lawyer. See contact info on inside back cover.</i>
<input type="checkbox"/> Contact information brokers.	<i>Information brokers buy criminal records and create criminal records files to sell to employers and debt collectors.</i> <input type="checkbox"/> Ask the law enforcement agency that arrested the thief for the names of information brokers who buy their records. <input type="checkbox"/> Write to the brokers and ask them to remove errors from your file.
<input type="checkbox"/> Update your files.	<input type="checkbox"/> Record the dates you made calls or sent letters. <input type="checkbox"/> Keep copies of letters in your files.

REDUCE YOUR RISK

Review Your Credit Reports

You have the right to get a free copy of your credit report every 12 months from each of the 3 nationwide credit reporting companies. Your credit report may show the first signs that someone has misused your information, so it's important to check your report a few times a year. Ordering 1 free report every 4 months lets you monitor your file and spot errors early.

You can get your free credit report at www.annualcreditreport.com or by calling 1-877-322-8228. You must give your name, address, Social Security number, date of birth, and the answers to questions that only you would know – for example, “How much is your monthly mortgage payment?” Each credit reporting company may ask you for different information. Use the form in the back of this book (page G1) to request your annual credit report by mail. For more information, visit www.ftc.gov/idtheft.

You also are entitled to a free copy of your credit report if:

- a company takes an adverse action against you, like denying your application for credit, insurance, or employment. You must ask for your report within 60 days of receiving notice of the adverse action. The notice will give you the name, address, and phone number of the credit reporting company to contact.
- you are unemployed and plan to look for a job within 60 days
- you are on public assistance
- your report is inaccurate because of fraud, including identity theft

Otherwise, a credit reporting company may charge you a fee for an additional copy of your report within a 12-month period. To buy a copy of your report, contact:

Equifax
1-800-685-1111
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-916-8800
www.transunion.com

Read Your Account and Billing Statements

- Look for charges you didn't make.
- Be alert for bills that don't arrive when you expect them.
- Follow up if you get credit card or account statements you don't expect.

Correct any errors as soon as possible.

Review Your Explanation of Medical Benefits

Call your medical insurer and health care provider if you see items that surprise you in your Explanation of Medical Benefits.

Respond Quickly to Notices from the Internal Revenue Service

If you get a notice from the IRS that suggests someone misused your Social Security number, respond quickly to the address included with the notice. The notice may say that you didn't pay taxes on a job you know you never held, or that your Social Security number was used on another return. Remember that the IRS never makes first contact with taxpayers by email, and doesn't ask for personal information through email. If you get email that claims to be from the IRS, call the IRS before you respond. Call 1-800-829-1040 for more information.

If you find out that an identity thief has used your Social Security number on a tax return, call the IRS's Specialized Identity Theft Protection Unit at 1-800-908-4490.

Identity Theft Protection Services

Should you pay a company to monitor your financial accounts, credit reports, and personal information? Many people find it valuable and convenient to pay a company for monitoring services. Other people choose to exercise their legal rights and protect their information for free. When you understand your rights, it can be easier to decide if you want to use a commercial service.

Before you buy an identity theft protection or monitoring product or service, get the details. Know exactly what you're paying for, as well as the total cost of the service.

Active Duty Alerts for Military Personnel

Military personnel have additional protections. If you're deployed, you can place an active duty alert on your credit reports to help minimize the risk of identity theft while you're away. Active duty alerts last for 1 year. If your deployment lasts longer, renew the alert.

HOW TO REQUEST AN ACTIVE DUTY ALERT

STEP BY STEP:	NOTES:			
<input type="checkbox"/> Contact 1 credit reporting company.	<table border="1" data-bbox="527 535 1468 630"><tr><td data-bbox="527 535 820 630">Equifax 1-800-525-6285</td><td data-bbox="820 535 1128 630">Experian 1-888-397-3742</td><td data-bbox="1128 535 1468 630">TransUnion 1-800-680-7289</td></tr></table> <ul data-bbox="535 651 1445 766" style="list-style-type: none"><input type="checkbox"/> Request an active duty alert.<input type="checkbox"/> Provide proof of identity, like a government-issued identity card, driver's license, military identification, birth certificate, or passport. <p data-bbox="535 777 1468 934"><i>The company you call must contact the others. The credit reporting companies will take your name off their marketing list for prescreened credit card offers for 2 years, unless you ask them to add you back onto the list.</i></p>	Equifax 1-800-525-6285	Experian 1-888-397-3742	TransUnion 1-800-680-7289
Equifax 1-800-525-6285	Experian 1-888-397-3742	TransUnion 1-800-680-7289		
<input type="checkbox"/> Mark your calendar.	<p data-bbox="535 966 1468 1039"><i>Active duty alerts last for 1 year. If your deployment lasts longer, renew the alert.</i></p>			
<input type="checkbox"/> Update your files.	<ul data-bbox="535 1081 1193 1165" style="list-style-type: none"><input type="checkbox"/> Record the dates you made calls or sent letters.<input type="checkbox"/> Keep copies of letters in your files.			