



Identity Recovery Toolkit



IDWISE

Brought to you by the Center for Identity
at The University of Texas at Austin

CONTENTS

- 2** My ID is missing or stolen
 - 2 Missing driver's license
 - 2 Missing passport
 - 2 Lost or stolen Social Security number or card
- 3** My mail was stolen
- 3** My financial information was stolen
 - 3 Create an Identity Theft Report
 - 5 Create an initial fraud alert and order your credit reports
 - 6 Request an extended fraud alert and consider a credit freeze
 - 7 Report any errors on your credit reports to credit agencies
 - 8 Consider an extended fraud alert
 - 8 Fraudulent activity on ATM or debit cards
 - 9 Fraudulent use of checking accounts
 - 9 Fraudulent use of credit cards
 - 10 Fraudulent use of investment accounts
 - 10 Find out if any bad checks have been written against your accounts
 - 11 Dispute fraudulent activity on existing accounts
 - 11 Bankruptcy
 - 12 Student loans
 - 12 Dealing with debt collectors
- 13** Someone stole or altered my medical information
 - 13 Get copies of your medical records if you suspect medical identity theft
 - 13 Contact health care providers and insurers
- 14** My tax records have been compromised
- 14** Monitor your identity
 - 14 Request your credit reports three times a year
 - 15 Review all account and billing statements
 - 15 Protect your personal information
- 16** Additional Resources
 - 16 Important Contact Info
 - 18 Credit Freeze Request Letter (Template)
 - 19 Dispute Letter for Existing Accounts (Template)
 - 20 Dispute Letter for Fraudulent New Accounts (Template)
 - 21 Dispute Letter to Credit Reporting Agency (Template)
 - 22 Notice to furnishers of information: obligation of furnishers under the FCRA

Discovering that you are the victim of identity theft can be frightening and overwhelming. In this toolkit, you will find concise and clear directions to quickly prevent further fraud and help you regain control over your identity.

MY ID IS MISSING OR STOLEN

If you are missing important identifying documents, you will need to file a report with the appropriate agency to replace them.

Missing driver's license

- » Contact the Department of Motor Vehicles (or the equivalent)
- » Cancel the lost license
- » Arrange for a replacement
- » Request a note be placed in your file so no one else can request an ID in your name
- » Make a note of the contacts in the [contact log](#)

Missing passport

The U.S. State Department's website has directions for reporting and re-issuing lost or stolen passports. <http://travel.state.gov/content/passports/english/passports/lost-stolen.html>
If you do not need to replace your passport, you can call 1-877-487-2278 (TTY 1-888-874-7793) to file a report.

Lost or stolen Social Security number or card

If you wish to replace a lost Social Security card, you can do so by following the directions at <https://faq.ssa.gov/ics/support/kbanswer.asp?deptID=34019&task=knowledge&questionID=1944>.

If this is the only type of identity theft you experienced, you may now move on to the "[Monitor your identity](#)" section. Otherwise, continue the recovery process.

MY MAIL WAS STOLEN

If you believe that your identity theft was the result of stolen mail, you should contact the U.S. Postal Inspection Service. You can find the address of the nearest office from your local post office, or at <https://postalinspectors.uspis.gov>. Record the dates of your contacts and letters.

If this is the only type of identity theft you experienced, you may now move on to the ["Monitor Your Identity" section](#). Otherwise, continue the recovery process.

MY FINANCIAL INFORMATION WAS STOLEN

Before you can begin dealing with the specific instances of financial identity theft, you'll need to create an Identity Theft Report.

Create an Identity Theft Report

GATHER YOUR INFORMATION.

Documents that can prove your unique identity will be crucial throughout the recovery process. Gather your Social Security card, driver's license, and utility bills. You will be asked to submit copies of these documents to a variety of people and organizations. Prepare multiple copies of each document in advance to make the process more efficient.

CREATE AN IDENTITY THEFT AFFIDAVIT WITH THE FEDERAL TRADE COMMISSION.

The Federal Trade Commission works closely with victims of identity theft to help law enforcement track down criminals. The FTC will collect details regarding your theft and refer complaints to other government agencies and businesses. You will produce an FTC affidavit during this process. It is a very important step in recovering your identity.

You can produce your affidavit in one of three ways:

ONLINE:

Complete the complaint form found at www.ftc.gov/complaint. Be sure to include as many details as you can.

- » Review the form and submit it.
- » Save the reference number that appears after submission. You will need it if you wish to update your complaint.
- » A prompt to print the affidavit will appear. Print the page immediately, as you will no longer have this option after leaving the screen.
- » Log the report in your [contact log](#).
- » If you need to update your report at any time, you can call the FTC at 1-877-438-4338 (TTY 1-866-653-4261).

BY PHONE:

- » Call the FTC at 1-877-438-4338 (TTY 1-866-653-4261).
- » Report the theft and all relevant details to a FTC representative.
- » Ask for your reference number and affidavit password.
- » The representative will email you a link to a site where you can print your affidavit. Follow the URL and enter your email address, password, and reference number.
- » Print and save the affidavit.
- » Log the call in your [contact log](#).
- » If you need to update your report at any time, call the FTC at 1-877-438-4338 (TTY 1-866-653-4261).

BY HAND:

- » A PDF version of the affidavit is available at <http://www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf>.
- » Download and print the form and complete it to the best of your ability. You do not need to mail it to the FTC; simply make multiple copies for your files.

CONTACT LOCAL LAW ENFORCEMENT

You can report identity theft to either your local police department or the business where the theft occurred. If you go to the police, we encourage you to follow the steps below:

- » Bring a copy of your FTC Identity Theft Affidavit.
- » Bring any additional proof of the theft that you may have (bank account statements, credit card statements, etc.).
- » Bring a government-issued photo ID.
- » Bring proof of your address, like a recent utility bill or lease agreement.
- » Bring along the FTC's "Memo to Law Enforcement," which can be downloaded at <http://www.consumer.ftc.gov/articles/pdf-0088-ftc-memo-law-enforcement.pdf>.
- » Complete and file a police report.
- » Ask for a copy of the report for your records. At a minimum, be sure to get the report number.
- » As always, record the dates and contact names from your visit in the [contact log](#) along with the report number.

COMPILE YOUR IDENTITY THEFT REPORT

An Identity Theft Report consists of the Federal Trade Commission's affidavit and your police report. You may need to submit both of these documents to a number of businesses and agencies, so please make several copies for your records.

Now that your Identity Theft Report is complete, you can move on to the steps to recover your financial identity.

Create an initial fraud alert and order your credit reports

Placing an initial fraud alert makes it difficult for identity thieves to open fraudulent accounts in your name. To do this, simply contact one of the three credit reporting agencies (or annualcredit-report.com), and ask that a fraud alert be placed on your account. This agency can then alert the other two on your behalf. When you place a fraud alert on your credit report, you are telling businesses that they must first verify your identity before responding to any credit requests.

Placing a fraud alert is completely free and the alert will remain in place for 90 days.

When requesting your fraud alert, take this opportunity to request your credit report. You are legally entitled to one free copy of your credit report a year with each of the three bureaus. Your credit report will show if the identity thieves have opened any fraudulent accounts in your name.

STEP-BY-STEP GUIDE TO CREATING AN INITIAL FRAUD ALERT:

- » Contact a credit reporting agency.
- » Explain that your identity has been stolen.
- » Ask for a fraud alert to be placed on your account.
- » Request that the company contact the other two credit reporting agencies on your behalf.
- » Mark your calendar to renew the fraud alert in 90 days.
- » Update your [contact log](#) to reflect the fraud alert request.
- » Copy any letters for your files.

CREDIT AGENCY CONTACT INFO

EQUIFAX

1-800-525-6285
www.equifax.com

EXPERIAN

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

TRANSUNION

1-800-680-7289

STEP-BY-STEP GUIDE FOR REQUESTING YOUR CREDIT REPORTS:

- » Contact all three credit reporting agencies and let them know you have requested a fraud alert.
- » Order your report, but request that only the last four digits of your Social Security number appear on it.
- » Update your [contact log](#) to reflect the fraud alert request.
- » Copy any letters for your files.

Request an extended fraud alert and consider a credit freeze

EXTENDED FRAUD ALERT:

Once you have created your Identity Theft Report, you are eligible for an extended fraud alert. An extended fraud alert stays in place for seven years and requires creditors to contact you by phone whenever an attempt is made to secure credit in your name. It also allows you to receive two free credit reports, within 12 months, from each of the nationwide credit reporting agencies. These reports allow you to closely monitor your credit.

In order to request the extended alert:

- » Separately contact all three credit reporting agencies.
- » Ask each agency to place an extended fraud alert on your file. You may be asked to complete a form.
- » Send a copy of your Identity Theft Report (affidavit and police report) with the completed form.
- » Mark your calendar to request your free credit reports, and for the end of the seven year period.
- » Add your requests to the [contact log](#).
- » Make copies of the request forms for your records.

CREDIT OR SECURITY FREEZE:

If you would like more control over your credit than what is offered with an extended fraud alert, you may consider requesting a security freeze. A security freeze prevents anyone other than you from accessing your credit report entirely, preventing any credit from being extended in your name. Security alerts are in effect until you request they be lifted, and should only be used if you will not need credit extended in the near future—for example, if you don't have plans to secure a car loan or open a new credit card. If you do need credit extended during the alert period, you can request a temporary lift.

To request a security freeze, you must use each agency's online process or submit a letter via certified mail. Your letter must include the following:

- » Full name, including middle initial and any suffixes, address, Social Security number, and date of birth
- » Any addresses where you have lived in the past five years
- » Proof of current address, such as utility bill or bank statement
- » A photocopy of a government-issued photo ID

You can use our [sample request letter](#) as a template.

Report any errors on your credit reports to credit agencies

Thoroughly review your credit reports. If you see any errors, like accounts you did not open or debts that do not belong to you, you will need to contact the credit reporting agencies to have them removed.

Follow these steps to dispute an error with a credit reporting agency:

- » Complete and send a copy of our [dispute letter](#) or your own letter via certified mail, to the credit reporting agency. The letter should include the following information:
 - › An explanation that you are a victim of identity theft
 - › A list of the errors that you found
 - › Documentation of the errors
 - › A request to remove the fraudulent information from your credit report
- » Wait for a response from the credit reporting agency. They must send a letter documenting any changes to your file, or an explanation of why they did not remove the information you requested.
- » Update your [contact log](#) and make copies of all communication with the agency.

When disputing fraudulent items on your credit report, the credit agency is required to report its findings to any businesses involved in the fraudulent items. The business then has 30 days to investigate and report findings back to the agency. If they find fraud, they will notify all credit reporting agencies, who can then remove the error. If no fraud is found, the credit reporting agencies will notify you of the findings.

Consider an extended fraud alert

If you haven't done so already, consider [placing an extended fraud alert](#) to continue to monitor for the creation of fraudulent accounts.

Fraudulent activity on ATM or debit cards

If your ATM or debit card has been compromised, acting quickly can save you time and money. Be sure to check your statements every month, and follow these steps if you lose your card, your card is stolen, or you notice a fraudulent transaction on your card:

- » Contact the card issuer and report the fraudulent transaction.
- » Send a follow-up letter to confirm your report. Use certified mail and request a return receipt for your records.
- » Record the date of the initial report, and the date the letter was mailed, in your [contact log](#).

YOUR MAXIMUM ATM OR DEBIT CARD LIABILITY, BY TIME OF REPORT:

Within two days of unauthorized transaction:
\$50

After two days but within 60 days of receiving a bank statement:
\$500

More than 60 days after receiving your bank statement:
Unlimited

Fraudulent use of checking accounts

Check fraud can occur in a variety of ways. Some of the most common are:

- » Check theft: the use of your stolen or lost checks
- » Checking account takeover: alterations to your account information in order for a thief to be able to use it
- » Check counterfeiting: producing fake checks with your account information

If you suspect that your checking account has been compromised, take the following steps to alleviate the damages:

- » Contact your bank or financial institution and request they stop payment on stolen checks or close your account.
- » Ask that your financial institution notify their check verification system so that businesses will refuse stolen checks.
- » Contact check verification companies on your own. Report the stolen check, or other checking account issue, and ask that businesses that use their service refuse checks on your account.
- » Make a record of all calls or letters sent in your [contact log](#).

If a bad check is passed in your name:

- » Contact the business that accepted the check and provide evidence of your identity theft before they begin collections against you.
- » Record the dates you called or sent letters in your [contact log](#).

Fraudulent use of credit cards

The Fair Credit Billing Act limits your liability for fraudulent credit card charges to \$50. However, reporting the card lost or stolen before any fraudulent charges occur can help eliminate this cost.

CHECK VERIFICATION COMPANIES

TELECHECK
1-800-710-9898

CERTEGY
1-800-437-5120

CHECK RITE
1-800-766-2748

CHEX SYSTEMS
1-800-428-9623

Please follow these steps to dispute fraudulent charges on your credit card:

- » Write to your credit card company, using our [simple template](#), or writing your own letter containing the following information:
 - › The amount and date of the billing error.
 - › Your name, address, and account number.
- » Mail the letter and a copy of your Identity Theft Report to the company's billing inquiry address, using certified mail with a return receipt request.
- » Patiently wait for the credit card company's response. They have up to 30 days to acknowledge your claim, and up to 90 days to resolve it.
- » Record dates of all calls and letters in your [contact log](#). Make copies of all letters for your files.

Fraudulent use of investment accounts

If you find any evidence of fraud in your investment or brokerage accounts, follow these steps to resolve the issue quickly:

- » Contact your account manager and explain the details of your situation to them
- » Contact the Securities and Exchange Commission:
 - › By phone: 1-800-732-0330
 - › Online: www.sec.gov/complaint.shtml
 - › By mail: SEC Office of Investor Education and Advocacy
100 F Street, NE
Washington, DC 20549
- » Update your [contact log](#) with dates and notes. Keep copies of any letters you sent.

Find out if any bad checks have been written against your accounts

If you believe fraudulent checks have been written from your account, contact your financial institution and carefully look over your banking statements. If you find fraudulent checks have been written, note the activity in your [account log](#) and ask your bank to close the account immediately.

If your checks have been stolen, or you find fraudulent activity on your checking account, you will also want to contact a check verification company. These companies provide businesses with the ability to quickly verify the validity of a check. Contacting them will make it difficult for a thief to use your checks in the future.

Three trusted verification companies are listed on page 16 and can help you. Call, report the theft, and ask them to inform businesses to refuse the stolen checks or checks written from the fraudulent account.

Dispute fraudulent activity on existing accounts

If you discover fraudulent activity on any of your existing accounts, you will need to take steps to dispute the charges with the financial institution involved. Follow the steps below when disputing charges:

- » Reset all passwords and PINs for your accounts. Make a note of the date of the change in the notes section of your [contact log](#).
- » Track down the dispute resolution address for the business; note it in your [account log](#).
- » Contact the dispute department and find out if they'll accept your Identity Theft Report. If not, request that the business send you the forms they use.
- » Complete and send a dispute letter to the business using certified mail. You can use [our template](#), or write your own that includes the following:
 - › An explanation that you are a victim of identity theft
 - › A list of the errors that you found
 - › Documentation of the errors
 - › A request to remove the fraudulent info from your account
- » Send a copy of your Identity Theft Report, or the forms required by the business, with your letter.
- » If the disputed items also appear on your credit report, send a copy, with any information not pertaining to the dispute blacked out.
- » Request a letter confirming that the fraudulent information has been removed. Save a copy of this letter for your files.
- » Update your [contact log](#) with relevant dates, and keep copies of all letters.

Bankruptcy

If someone files bankruptcy in your name, you will need to contact the U.S. Trustee in the region where the filing was made. Regional office listings are at www.usdoj.gov/ust.

Send a letter to the Trustee explaining the situation. Be sure to include proof of your identity.

It may be necessary to hire an attorney to explain the fraudulent filing to the court. You can contact your state Attorney General to get information about lawyer referral services in your state. A list of Attorney General websites is at <http://www.naag.org/current-attorneys-general.php>.

As always, [log your calls](#) and letters and keep copies of any mail you send.

Student loans

If your credit report reflects fraudulent student loans, you will need to contact the school or program that issued the loan and ask them to close it. In addition, you should contact the U.S. Department of Education and also provide documentation of the fraud to them.

U.S. DEPARTMENT OF EDUCATION

[www.ed.gov/about/offices/list/
oig/hotline.html](http://www.ed.gov/about/offices/list/oig/hotline.html)
1-800-647-8733

Dealing with debt collectors

Debt collectors and collection agencies may contact you if an identity thief incurs debt in your name but fails to make payments. This can be especially stressful. You will need to follow the steps below to stop the calls or letters, and quickly end any collection efforts against you.

Office of the Inspector General
400 Maryland Avenue, SW
Washington, DC 20202

- » Within 30 days of notice of the debt, write to the debt collector. Indicate that you are a victim of identity theft, and include a copy of your Identity Theft Report. Be sure to send the letter certified mail, with return receipt.
- » The collector must stop any collection efforts against you until it verifies the debt and notify the company that incurred the debt that you are an identity theft victim.
- » In the same or a separate letter, request the debt collector to stop contacting you. A debt collector is only allowed one additional contact after receiving such a letter—either to acknowledge that they won't contact you again, or to outline the specific action that they intend to take.
- » Contact the business where the debt was incurred, explain that it is not your debt, and request any documentation related to the debt (credit card receipts, credit card applications, etc.).
- » Contact all three credit reporting agencies. Include copies of your Identity Theft Report, and ask that they block the fraudulent information from your credit report. You can use [our sample letter](#).
- » Record all calls and letters mailed in your [contact log](#) and keep copies and notes for your files.

If this is the only type of identity theft you experienced, you may now move on to the "[Monitor Your Identity](#)" section. Otherwise, continue the recovery process.

SOMEONE STOLE OR ALTERED MY MEDICAL INFORMATION

Get copies of your medical records if you suspect medical identity theft

Medical identity theft is an increasing problem. It is important to take care of any identity theft related to medical treatment immediately. If a thief uses your name or Social Security number to receive medical treatment, his or her medical information can compromise your personal medical file.

Contact your doctor, explain the situation, and request copies of your medical records. There may be fees associated with this process. If your medical provider refuses to give you copies, contact the person listed on the Notice of Privacy Practices or the practice's patient representative. If you are still unable to retrieve your records, contact the U.S. Department of Health and Human Services Office for Civil Rights (www.hhs.gov/ocr). They will be able to help you.

Review your records carefully, and note any fraudulent activity in the [account log](#).

Contact health care providers and insurers

Medical identity theft is particularly dangerous because it can affect your ability to receive necessary treatment, as well as compromise the accuracy of the information contained within your medical files.

Using the medical records you have requested, follow these steps to alleviate medical identity theft and reduce the risks to your health information:

- » Carefully review your medical records. Report any errors to your medical provider.
- » Send a letter to your both your healthcare provider and your health insurance carrier.
 - › In the letter, explain the error, and ask that your file be updated to only include accurate information. Include a copy of your Identity Theft Report.
 - › Mail the letters via certified mail, with return receipt. You should receive a reply within 30 days.
 - › Update your [contact log](#) and files accordingly.
- » Notify the credit reporting agencies of the issue.
- » If you haven't already, review your credit reports for any medical debts.
- » Update your records.

If this is the only type of identity theft you experienced, you may now move on to the "[Monitor Your Identity](#)" section. Otherwise, continue the recovery process.

MY TAX RECORDS HAVE BEEN COMPROMISED

If you have experienced tax ID theft, you will need to begin by completing an ID Theft Report. You can follow the directions in the [financial identity theft section](#) of this document to do so.

Once the report is complete, follow these instructions to repair the damage.

Income tax fraud can occur in a variety of ways. If someone uses your Social Security number to seek employment, their employer will report wages to the IRS, but you will not report those on your tax return. If someone uses your Social Security number to file a tax return, they may be able to collect a refund. In either case, when you file your return using the same number you will receive a letter from the IRS indicating that your Social Security number has been used by someone else.

If you suspect either of these scenarios has occurred, you should contact the IRS and work with a tax fraud specialist, following these steps:

- » Contact the IRS Identity Protection Specialized Unit:
 - › 1-800-908-4490
 - › www.irs.gov/identitytheft
- » Report the fraud, and request and complete IRS form 14039.
- » Send the IRS a copy of your police report and form 14039, along with proof of your identity, such as driver's license or passport.
- » Update your [contact log](#) and make copies for your file.

MONITOR YOUR IDENTITY

Now that you have accomplished these tasks to recover your identity, we hope you feel in control of this stressful situation. We encourage you to adopt proactive habits that will keep your identity safe in the future.

Request your credit reports three times a year

You can get a free copy of your credit report from each of the three nationwide credit reporting agencies once a year. Mark your calendar to request one report every four months. Free reports can be requested from www.annualcreditreport.com.

Review all account and billing statements

Be on the lookout for suspicious charges or bills for accounts you are unfamiliar with, and use the steps in this document to eliminate the problems.

Protect your personal information

- » Keep important papers and laptops secure. Consider investing in a safe for storing documents at home, and carry only what is absolutely necessary outside of your home. Shred documents that you no longer need before putting them in the trash.
- » Protect your Social Security number, and those of your family members. If someone requests your Social Security number, ask if they can use a different form of identification. If they cannot, ask for clarification on why they need it, how it will be used, and how it will be safe-guarded.
- » Be smart about online interaction. Never respond to email requests for personal information. If you have concerns, call the company and verify that the request is legitimate.
- » Protect your computers with anti-virus and firewall software. Do not open email attachments, or click on links, from unknown senders.
- » Properly remove all personal information from your computer or mobile device before discarding it.
- » Use strong passwords, and change them regularly.
- » Think carefully about the information you share via social networks. Take the time to understand the privacy policies and settings of the sites you use.

ADDITIONAL RESOURCES

Important Contact Info

OPT OUT

To opt out of prescreened credit and insurance offers:

www.optoutprescreen.com

1-888-567-8688

FREE ANNUAL CREDIT REPORTS

www.annualcreditreport.com

1-877-322-8228

CREDIT REPORTING AGENCIES

Equifax

www.equifax.com

1-800-525-6285

Experian

www.experian.com

1-888-397-3742

TransUnion

www.transunion.com

1-800-680-7289

CHECK VERIFICATION COMPANIES

Certegy

www.askcertegy.com

1-800-437-5120

ChexSystems, Inc.

www.consumerdebit.com

1-800-428-9623

TeleCheck Services, Inc.

www.firstdata.com/telecheck

1-800-710-9898

FEDERAL AGENCIES

Federal Communications Commission

www.fcc.gov/cgb

1-888-225-5322

1-888-835-5322 (TTY)

Federal Financial Institutions Examination Council
www.ffiec.gov/consumercenter

Federal Trade Commission
www.ftc.gov/complaint
1-877-438-4338
1-866-653-4261 (TTY)

Internal Revenue Service
Identity Protection Specialized Unit
www.irs.gov/identitytheft
1-800-908-4490

Legal Services Programs
www.lsc.gov/local-programs/program-profiles

Social Security Administration
To report fraud: go to www.socialsecurity.gov and type "Fraud" in the Search box.
1-800-269-0271
1-866-501-2101 (TTY)

U.S. Department of Education
www.ed.gov/about/offices/list/oig/hotline.html
1-800-647-8733

U.S. Department of Justice
www.justice.gov/ust/eo/fraud
USTP.Bankruptcy.Fraud@usdoj.gov

U.S. Postal Inspection Service
<https://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx>
1-877-876-2455

U.S. Postal Service
www.usps.com/holdmail
www.usps.com
1-800-275-8777

U.S. Securities and Exchange Commission
www.sec.gov/complaint/tipscomplaint.shtml
1-800-732-0330

U.S. Department of State
www.travel.state.gov/passport
1-877-487-2778
1-888-874-7793 (TDD/TTY)

Credit Freeze Request Letter (Template)

[Your Name]
[Your Address]
[Your City/State/Zip]

[Date]

[Credit Reporting Agency Name]
[Credit Reporting Agency Address]

Re: Request for credit freeze

I am a victim of identity theft. As such, I request that you please place an extended seven-year fraud alert on my credit report. In addition, please remove the first five digits of my Social Security number from my report, and add the following statement: FRAUD VICTIM! DO NOT EXTEND CREDIT WITHOUT CONTACTING ME PERSONALLY. MY DAYTIME PHONE NUMBER IS [XXX-XXX-XXXX].

I am enclosing a copy of my law enforcement report of the identity theft, my Identity Theft Affidavit, and my identification for your convenience. Please do not hesitate to contact me if I can provide additional information.

Sincerely,

[Your Signature]
[Your Printed Name]

Enclosures:

Law Enforcement Report
Identity Theft Affidavit
Copy of Identification

Dispute Letter for Existing Accounts (Template)

[Your Name]
[Your Address]
[Your City/State/Zip]

[Date]

[Name of Company]
ATTN: [Collections, Fraud Department, or Billing Inquiries]
[Address]
[City, State, Zip Code]

Re: [Account Number]

I am a victim of identity theft. As such, I am writing to dispute the following fraudulent charges on my account. I did not initiate or authorize these charges:

[Transaction Description] [Transaction Date] [Transaction Amount]

I request that you remove the fraudulent charges as well as any finance or other related charges from my account, send me an updated statement, and **close the account (if applicable)**. I also request that you stop reporting this inaccurate information and report the revised, correct information to all three credit reporting agencies.

I am enclosing a copy of my law enforcement report of the identity theft, my Identity Theft Affidavit, and my identification for your convenience. Additionally, I've enclosed a copy of my account statement showing the fraudulent charges and a credit report showing the information requiring updating. Also enclosed is a copy of the Federal Trade Commission Notice to Furnishers of Information. This document outlines your responsibilities under the Fair Credit Reporting Act.

Please send me a written report of your findings and actions once your investigation is complete, and please do not hesitate to contact me if I can provide additional information.

Sincerely,

[Your Signature]
[Your Printed Name]

Enclosures:

Law Enforcement Report
Identity Theft Affidavit
Account Statement identifying fraudulent information
Credit Report
[FTC Notice to Furnishers of Information](#)
Copy of Identification

Dispute Letter for Fraudulent New Accounts (Template)

[Your Name]
[Your Address]
[Your City/State/Zip]

[Date]

[Name of Company]
ATTN: [Collections, Fraud Department, or Billing Inquiries]
[Address]
[City, State, Zip Code]

Re: [Account Number]

I recently found out that an account has been opened at your business using my personal information. I am a victim of identity theft and did not request or authorize this account. Please close it immediately. Additionally, I request that [Name of Company] absolve me of any responsibility and charges for the account, and that you contact the appropriate companies to have the fraudulent information removed from my credit reports.

I've enclosed a copy of my law enforcement report, an Identity Theft Affidavit, evidence of my identity, and a copy of my credit report showing the fraudulent items. I've also included a copy of the Federal Trade Commission Notice to Furnishers of Information. This document states your responsibilities as an information furnisher to credit reporting companies (CRCs). As such, you are required to stop furnishing any information resulting from the identity theft to any credit reporting company upon receipt of this written request. Under section 605B of the Fair Credit Reporting Act, your responsibilities also include no longer providing the inaccurate information to any CRC, and guaranteeing that the fraudulent debts are not sold or transferred to another party for collection.

I request that you close the account, absolve any charges, fully investigate the matter, adhere to the Fair Reporting Act's requirements, and send me a follow-up letter outlining your conclusions and the actions you have taken.

Sincerely,

[Your Signature]
[Your Printed Name]

Enclosures:

Law Enforcement Report
Identity Theft Affidavit
Account Statement identifying fraudulent information
Credit Report
FTC Notice to Furnishers of Information
Copy of Identification

Dispute Letter to Credit Reporting Agency (Template)

[Your Name]
[Your Address]
[Your City/State/Zip]

[Date]

[Credit Reporting Agency Name]
[Credit Reporting Agency Address]

Re: Dispute of information on credit report

I am a victim of identity theft. As such, I am writing to dispute certain information that currently occurs on my credit report as a result of the crime. The following fraudulent inquiries or accounts related to transactions not initiated or authorized by me:

[Company Name or Court Info] [Description of fraudulent information, like "Account", or "Judgment"]

As required by the Fair Credit Reporting Act, I am requesting that these items be removed [or request another change] because they are attributable to identity theft. If you do not remove the entries, please provide proof of your reason for non-removal.

I am enclosing a copy of my law enforcement report of the identity theft, my Identity Theft Affidavit, and my identification for your convenience. Additionally, I've enclosed a copy of my credit report from your agency with the fraudulent items highlighted.

Please do not hesitate to contact me if I can provide additional information.

Sincerely,

[Your Signature]
[Your Printed Name]

Enclosures:

Law Enforcement Report
Identity Theft Affidavit
Credit Report identifying fraudulent information
Copy of Identification

Notice to furnishers of information: obligation of furnishers under the FCRA

All furnishers subject to the Federal Trade Commission's jurisdiction must comply with all applicable regulations, including regulations promulgated after this notice was prescribed in 2004. Information about applicable regulations currently in effect can be found at the Commission's Web site, www.ftc.gov/credit. Furnishers who are not subject to the Commission's jurisdiction should consult with their regulators to find any relevant regulations.

NOTICE TO FURNISHERS OF INFORMATION: OBLIGATIONS OF FURNISHERS UNDER THE FCRA

The federal Fair Credit Reporting Act (FCRA), 15 U.S.C. 1681-1681y, imposes responsibilities on all persons who furnish information to consumer reporting agencies (CRAs). These responsibilities are found in Section 623 of the FCRA, 15 U.S.C. 1681s-2. State law may impose additional requirements on furnishers. All furnishers of information to CRAs should become familiar with the applicable laws and may want to consult with their counsel to ensure that they are in compliance. The text of the FCRA is set forth in full at the Web site of the Federal Trade Commission (FTC): www.ftc.gov/credit. A list of the sections of the FCRA crossreferenced to the U.S. Code is at the end of this document.

Section 623 imposes the following duties upon furnishers:

ACCURACY GUIDELINES

The banking and credit union regulators and the FTC will promulgate guidelines and regulations dealing with the accuracy of information provided to CRAs by furnishers. The regulations and guidelines issued by the FTC will be available at www.ftc.gov/credit when they are issued. Section 623(e).

GENERAL PROHIBITION ON REPORTING INACCURATE INFORMATION

The FCRA prohibits information furnishers from providing information to a CRA that they know or have reasonable cause to believe is inaccurate. However, the furnisher is not subject to this general prohibition if it clearly and conspicuously specifies an address to which consumers may write to notify the furnisher that certain information is inaccurate. Sections 623(a)(1)(A) and (a)(1)(C).

DUTY TO CORRECT AND UPDATE INFORMATION

If at any time a person who regularly and in the ordinary course of business furnishes information to one or more CRAs determines that the information provided is not complete or accurate, the furnisher must promptly provide complete and accurate information to the CRA. In addition, the furnisher must notify all CRAs that received the information of any corrections, and must thereafter report only the complete and accurate information. Section 623(a)(2).

DUTIES AFTER NOTICE OF DISPUTE FROM CONSUMER

If a consumer notifies a furnisher, at an address specified for the furnisher for such notices, that specific information is inaccurate, and the information is, in fact, inaccurate, the furnisher must thereafter report the correct information to CRAs. Section 623(a)(1)(B).

If a consumer notifies a furnisher that the consumer disputes the completeness or accuracy of any information reported by the furnisher, the furnisher may not subsequently report that information to a CRA without providing notice of the dispute. Section 623(a)(3).

The federal banking and credit union regulators and the FTC will issue regulations that will identify when an information furnisher must investigate a dispute made directly to the furnisher by a consumer. Once these regulations are issued, furnishers must comply with them and complete an investigation within 30 days (or 45 days, if the consumer later provides relevant additional information) unless the dispute is frivolous or irrelevant or comes from a "credit repair organization." The FTC regulations will be available at www.ftc.gov/credit. Section 623(a)(8).

DUTIES AFTER NOTICE OF DISPUTE FROM CONSUMER REPORTING AGENCY

If a CRA notifies a furnisher that a consumer disputes the completeness or accuracy of information provided by the furnisher, the furnisher has a duty to follow certain procedures. The furnisher must:

- Conduct an investigation and review all relevant information provided by the CRA, including information given to the CRA

by the consumer. Sections 623(b)(1)(A) and (b)(1)(B).

- Report the results to the CRA that referred the dispute, and, if the investigation establishes that the information was, in fact, in- complete or inaccurate, report the results to all CRAs to which the furnisher provided the information that compile and maintain files on a nationwide basis. Section 623(b)(1)(C) and (b)(1)(D).
 - Complete the above steps within 30 days from the date the CRA receives the dispute (or 45 days, if the consumer later provides relevant additional information to the CRA). Section 623(b)(2).
 - Promptly modify or delete the information, or block its reporting. Section 623(b)(1)(E).

DUTY TO REPORT VOLUNTARY CLOSING OF CREDIT ACCOUNTS

If a consumer voluntarily closes a credit account, any person who regularly and in the ordinary course of business furnishes information to one or more CRAs must report this fact when it provides information to CRAs for the time period in which the account was closed. Section 623(a)(4).

DUTY TO REPORT DATES OF DELINQUENCIES

If a furnisher reports information concerning a delinquent account placed for collection, charged to profit or loss, or subject to any similar action, the furnisher must, within 90 days after reporting the information, provide the CRA with the month and the year of the commencement of the delinquency that immediately preceded the action, so that the agency will know how long to keep the information in the consumer's file. Section 623(a)(5).

Any person, such as a debt collector, that has acquired or is responsible for collecting delinquent accounts and that reports information to CRAs may comply with the requirements of Section 623(a)(5) (until there is a consumer dispute) by reporting the same delinquency date previously reported by the creditor. If the creditor did not report this date, they may comply with the FCRA by establishing reasonable procedures to obtain and report delinquency dates, or, if a delinquency date cannot be reasonably obtained, by following reasonable procedures to ensure that the date reported precedes the date when the account was placed for collection, charged to profit or loss, or subjected to any similar action. Section 623(a)(5).

DUTIES OF FINANCIAL INSTITUTIONS WHEN REPORTING NEGATIVE INFORMATION

Financial institutions that furnish information to "nationwide" consumer reporting agencies, as defined in Section 603(p), must notify consumers in writing if they may furnish or have furnished negative information to a CRA. Section 623(a)(7). The Federal Reserve Board has prescribed model disclosures, 12 CFR Part 222, App. B.

DUTIES WHEN FURNISHING MEDICAL INFORMATION

A furnisher whose primary business is providing medical services, products, or devices (and such furnisher's agents or assignees) is a medical information furnisher for the purposes of the FCRA and must notify all CRAs to which it reports of this fact. Section 623(a)(9). This notice will enable CRAs to comply with their duties under Section 604(g) when reporting medical information.

DUTIES WHEN ID THEFT OCCURS

All furnishers must have in place reasonable procedures to respond to notifications from CRAs that information furnished is the result of identity theft, and to prevent refurnishing the information in the future. A furnisher may not furnish information that a consumer has identified as resulting from identity theft unless the furnisher subsequently knows or is informed by the consumer that the information is correct. Section 623(a)(6). If a furnisher learns that it has furnished inaccurate information due to identity theft, it must notify each consumer reporting agency of the correct information and must thereafter report only complete and accurate information. Section 623(a)(2). When any furnisher of information is notified pursuant to the procedures set forth in Section 605B that a debt has resulted from identity theft, the furnisher may not sell, transfer, or place for collection the debt except in certain limited circumstances. Section 615(f).

The FTC's Web site, www.ftc.gov/credit, has more information about the FCRA, including publications for businesses and the full text of the FCRA.