

# **ID THEFT PREVENTION & INFORMATION**

**You are a victim of identity theft; there are a number of important steps for you to follow. Be prepared to document all unauthorized transactions and to be patient. The process can take a number of months.**

**In most cases, the uniform officer that filled out a report is not the investigating officer. Your report number is:\_\_\_\_\_.**

**The following information in this packet will assist you in contacting various agencies. Complete the necessary forms and document everything you do. This case will be assigned to an investigator. In a short time he or she will be contacting you for an interview. It is important that you follow the instructions in this packet and make every effort to complete each form.**

**Step 1 - Contact your bank and other credit card issuers. If the theft involved existing bank accounts (checking and saving accounts as well as credit or debit cards) you should take the following steps:**

- Put stop payment orders on all outstanding checks that might have been written without your knowledge or permission.
- Close all existing credit card accounts and any account accessible by debit card.
- Open up new accounts protected with a secret password or personal identification number (PIN). **Do not use the same passwords or PINs as on the original accounts.**

**Do not use common numbers (like birth dates, part of your social security number) or commonly chosen words (such as a child, spouse or pet's name) as passwords or PINs.**

**Step 2 - File a report with the Federal Trade Commission.** You can go on-line to file an identity theft complaint with the F.T.C. at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). There is an ID Theft Affidavit enclosed in this packet. Many creditors and major credit reporting bureaus will accept the "ID Theft Affidavit" available on this F.T.C. web-site. Go to <http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>. If you file on-line be sure to make a copy for the investigator that will be contacting you.

**Step 3 - Contact all three major credit reporting bureaus.** First request the credit bureaus to place a "fraud alert" on your file. You must then be contacted directly before any new credit is taken out in your name. Second, file your police report or the report number given to you by the police and file it immediately with the credit reporting bureaus. A fraud report will be shared with the other bureaus. Place a security freeze on your credit reports. By contacting the three credit bureaus by letter or Internet you will be assigned a "PIN" number that can only be unlocked.

Scamsafe.com - will give you instructions on how to do a security freeze.

You can contact the fraud units at each of the bureaus as follows:

Equifax  
P.O. Box 740256  
Atlanta, GA 30374  
Consumer Fraud Division  
800/525-6285

Experian  
P.O. Box 2002  
Allen, TX 75013  
National Consumer Assistance  
888/397-3742

TransUnion  
P.O. Box 6790  
Fullerton, CA 92834  
Fraud Victim Assistance Dept.  
800/680-7289

**Step 4 - Contact all of your creditors by phone and in writing.** File a law enforcement report, or the F.T.C.'s ID Theft Affidavit, with each creditor. (Some may require that you use their own form of an affidavit.)

Keep copies of all correspondence and documents exchange with each creditor. An Identity Theft Checklist and Journal are enclosed in this packet to assist you.

Cancel all existing credit card accounts and open replacement accounts. Ask that those canceled accounts be processed as "account closed at customer's request" to avoid any negative reporting to credit bureaus.

**Step 5 - Notify the phone company.** If the identity theft involves the misuse of a long-distance telephone account, cellular telephone, or other telephone service, contact your telephone or wireless company and immediately close all existing accounts.

**Step 6 - Notify the post office.** If you suspect that your mail has been stolen or diverted with a false change-of-address request, contact your local postal inspector. You can obtain the address and telephone number of your local postal inspector by visiting the United States Postal Service web site at:  
<http://www.usps.com/ncsc/locators/findis.html>.

**Step 7 - Notify the Social Security Administration.** If you suspect that someone is using your social security number to obtain credit or employment, contact the Social Security Administration's fraud hotline at 1-800-269-0271. To check the accuracy of your work history, order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) and check it for accuracy. You can obtain the PEBES application at your local Social Security office or you can download one from the Social Security Administration web site: <http://www.ssa.gov/online/ssa-7004.pdf>.

**Step 8 - Notify the State Department.** If your passport has been stolen, notify the passport office in writing to be on guard for anyone ordering a new passport in your name. You can obtain additional information from their web site: <http://travel.state.gov/reportppt.html>.

**Step 9 - If you are contacted by a collection agency** about a debt for which you are not responsible, immediately notify them that you did not create the debt and that you are a victim of identity theft. Follow up with the collection agency and creditor in writing and include a copy of your police report or ID Theft Affidavit.

Send all letters and copy of the report affidavits "Return Receipt Requested" or with some other process that gives you proof that the collection agency received your letter.

**Step 10 - This is one of your most important steps.** Record everything. Make copies of everything. Leave nothing out. Get names and numbers of people you have contacted. Use the forms enclosed in this packet to assist you.

- The assigned detective wants to put the criminal in jail.
- The person that knows the details and facts of the case is you.
- By not filling out the victim packet, the result is the assigned detective may determine that the case is not workable.
- Detectives have heavy caseloads.
- Your case is not the only case he or she is working.
- When you come in for the interview, bring everything.
- Listen to the questions asked and direct your answers to those questions.
- Remember. The detective is in charge of the case.
- Respect their time and be brief during phone calls you make to them.
- Rudeness never works.
- Identity theft cases are slow and may take months to complete. It's not like what you see on TV.
- Leads may not pan out and evidence that you think might be perfect doesn't always prove a case.

Following is a list of contacts you may need to make. Remember, usually you can get this information faster than the detective because you don't need a subpoena. He would.

# CONSUMER SENTINEL'S IDENTITY THEFT DATA CLEARINGHOUSE

## Identity Theft...An Insidious Crime

ID thieves steal personal information, such as a credit card account number, Social Security number or driver's license number. Then they open up accounts in a consumer's name and run up charges on the account. Or, they use the personal information to charge goods and services to a consumer's existing accounts. In other cases, they may work, or even be arrested, while using the victim's name.

The harm to a consumer's credit and daily life can be devastating. Victims of ID theft often have trouble getting new credit cards or loans because of the damage to their credit ratings.

According to the ID Theft Data Clearinghouse, the most common types of identity theft are:

- using or opening a credit card account fraudulently
- opening telecommunications or utility accounts fraudulently
- passing bad checks or opening a new bank account
- getting loans in another person's name
- working in another person's name.

## What to Tell Victims of Identity Theft:

1. Contact the fraud departments of each of the three major credit bureaus, report the theft, ask that a "fraud alert" be placed on their file and that no new credit be granted without their approval.
  - Equifax: 1.800.525.6285
  - Experian: 1.888.397.3742
  - Trans Union: 1.800.680.7289
2. For any accounts that have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions. Close these accounts. Put passwords (not mother's maiden name or Social Security number) on any new accounts they open.
3. File a report with local police or the police where the identity theft took place. Get the report number or a copy of the report in case the bank, credit card company or others need proof of the crime later.
4. Call the ID Theft Clearinghouse toll-free at **1.877.ID.THEFT (1.877.438.4338)** to report the theft. Counselors will take their complaint and advise them on how to deal with the credit-related problems that could result from ID theft. The Identity Theft Hotline and the ID Theft Website ([www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)) give consumers one place to report the theft to the federal government and receive helpful information.

## The Cybertool for ID Theft Investigations

### Investigating Identity Theft?

The **Identity Theft Data Clearinghouse** is an essential tool for law enforcement. As the nation's repository for identity theft complaints, the Clearinghouse offers law enforcement officers:

- access to the nation's only central database of identity theft complaints
- information on trends in identity theft
- an opportunity to work with other law enforcement agencies and appropriate private organizations—from their own desktop computer.

The Identity Theft Data Clearinghouse is part of Consumer Sentinel, an online cybertool and fraud complaint database used by hundreds of civil and criminal law enforcement agencies in the United States and abroad. To access the Clearinghouse, contact the Consumer Sentinel project team at **1.877.701.9595**. The Federal Trade Commission (FTC) manages and maintains the Clearinghouse and Consumer Sentinel.

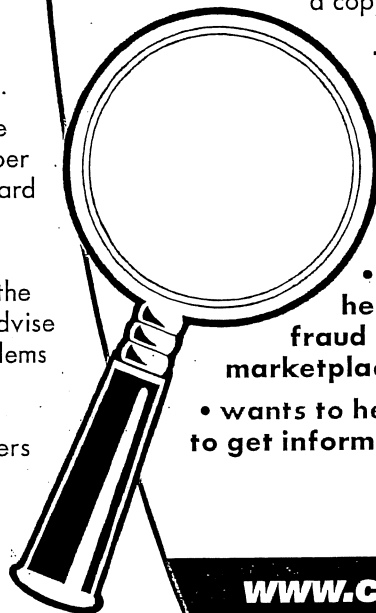
Consumer Sentinel

## ID Theft Affidavit Simplifies Reporting for Consumers

The *ID Theft Affidavit* makes it easier for consumers to dispute debts resulting from identity theft. The *ID Theft Affidavit* is accepted by the three major credit bureaus, participating credit issuers and other financial institutions. Log on to [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or call **1.877.ID.THEFT** for a copy of the *ID Theft Affidavit*.

The Federal Trade Commission, the nation's consumer protection champion:

- enforces federal laws that protect consumers.
- provides free information to help consumers spot and avoid fraud and deception in the marketplace.
- wants to hear from consumers who want to get information or file a complaint.



**1.877.ID.THEFT**

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)



# Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

## What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.



## Know the warning signs

In tax-related identity theft, the criminal generally will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season.

You may be unaware that this has happened until you file your return later in the filing season and discover that two returns have been filed using the same SSN.

Be alert to possible identity theft if you receive an IRS notice or letter that states:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages from an employer unknown to you.

## Steps for victims of identity theft

1. File a report with the local police.
2. File a complaint with the Federal Trade Commission at [www.identitytheft.gov](http://www.identitytheft.gov) or the FTC Identity Theft Hotline at 1-877-438-4338 or TTY 1-866-653-4261.
3. Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - [www.Equifax.com](http://www.Equifax.com) 1-800-525-6285
  - [www.Experian.com](http://www.Experian.com) 1-888-397-3742
  - [www.TransUnion.com](http://www.TransUnion.com) 1-800-680-7289

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, take these additional steps:

4. Respond immediately to any IRS notice; call the number provided

5. Complete IRS Form 14039, Identity Theft Affidavit. Use a fillable form at [IRS.gov](http://IRS.gov), print, then mail or fax according to instructions.

6. Continue to pay your taxes and file your tax return, even if you must do so by paper.

If you previously contacted the IRS and did not have a resolution, contact the Identity Protection Specialized Unit at 1-800-908-4490. We have teams available to assist.

More information: [www.irs.gov/identitytheft](http://www.irs.gov/identitytheft) or FTC's [www.identitytheft.gov](http://www.identitytheft.gov).

## About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft."

## How you can reduce your risk

- Don't routinely carry your Social Security card or any document with your SSN on it.
- Don't give a business your SSN just because they ask – only when absolutely necessary.
- Protect your personal financial information at home and on your computer.
- Check your credit report annually.
- Check your Social Security Administration earnings statement annually.
- Protect your personal computers by using firewalls, anti-spam/virus software, update security patches and change passwords for Internet accounts.
- Don't give personal information over the phone, through the mail or the Internet unless you have either initiated the contact or are sure you know who is asking.

**NOTE:** The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

<b>Form 14039</b> Rev. February 2014	Department of the Treasury - Internal Revenue Service <b>Identity Theft Affidavit</b>	<b>OMB Number</b> 1545-2139
---	--	--------------------------------

**Section E – Representative Information** (Required only if completing this form on someone else's behalf)

If you are completing this form on behalf of another person, you **must** complete this section **and** attach **clear and legible** photocopies of the documentation indicated.

Check only **ONE** of the following four boxes next to the reason why you are submitting this form

- ☐ The taxpayer is deceased and I am the surviving spouse. (*No attachments are required*)
- ☐ The taxpayer is deceased and I am the court-appointed or certified personal representative.  
Attach a copy of the court certificate showing your appointment.
- ☐ The taxpayer is deceased and a court-appointed or certified personal representative has not been appointed.  
Attach a copy of the death certificate or the formal notification from the appropriate government office informing the next of kin of the decedent's death. Indicate your relationship to the decedent: \_\_\_\_\_
- ☐ The taxpayer is unable to complete this form and I have been appointed conservator or have Power of Attorney (POA) authorization.  
Attach a copy of the documentation showing your appointment as conservator or your POA authorization.  
If you are the POA and have been issued a CAF number by the IRS, enter it here: \_\_\_\_\_

Representative's name \_\_\_\_\_

Current mailing address \_\_\_\_\_

City _____	State _____	ZIP code _____
------------	-------------	----------------

**Section F – Penalty Of Perjury Statement and Signature** (Required for all filers)

Under penalty of perjury, I declare that, to the best of my knowledge and belief, the information entered on this form is true, correct, complete, and made in good faith.

Signature of taxpayer or representative of taxpayer _____	Date signed _____
---	-------------------

**Instructions for Submitting this Form**

Submit this form and **clear and legible** copies of required documentation using **ONE** of the following submission options.

Mailing **AND** faxing this form **WILL** result in a processing delay.

By Mail	By FAX
<p>If you checked Box 1 in Section A and are unable to file your return electronically because the primary and/or secondary SSN was misused, attach this form and documentation to your paper return and submit to the IRS location where you normally file. <b>If you have already filed your paper return</b>, submit this form and documentation to the IRS location where you normally file. Refer to the "Where Do You File" section of your return instructions or visit IRS.gov and input the search term "Where to File".</p> <p>If you checked Box 1 in Section A and are submitting this form in response to a notice or letter received from the IRS, return this form and documentation with a copy of the notice or letter to the address contained in the notice or letter.</p> <p>If you checked Box 2 in Section A (you do not currently have a tax-related issue), mail this form and documentation to:</p> <p style="text-align: center;">Internal Revenue Service PO Box 9039 Andover MA 01810-0939</p>	<p>If you checked Box 1 in Section A and are submitting this form in response to a notice or letter received from the IRS that shows a reply FAX number, FAX this completed form and documentation with a copy of the notice or letter to that number. Include a cover sheet marked "Confidential." If no FAX number is shown, follow the mailing instructions on the notice or letter.</p> <p>If you checked Box 2 in Section A (you do not currently have a tax-related issue), FAX this form and documentation to: (855) 807-5720.</p> <p><b>NOTE:</b> The IRS does not <i>initiate</i> contact with taxpayers by email, fax, or any social media tools to request personal or financial information. Report unsolicited email claiming to be from the IRS and bogus IRS websites to <a href="mailto:phishing@irs.gov">phishing@irs.gov</a>.</p> <p><b>NOTE:</b> For more information about questionable communications purportedly from the IRS, visit IRS.gov and input the search term "Fake IRS Communications".</p>

Other helpful identity theft information may be found on [www.irs.gov/uac/Identity-Protection](http://www.irs.gov/uac/Identity-Protection). Additionally, locations and hours of operation for Taxpayer Assistance Centers can be found at [www.irs.gov](http://www.irs.gov) (search "Local Contacts").

**Note:** The Federal Trade Commission (FTC) is the central federal government agency responsible for identity theft awareness. The IRS does not share taxpayer information with the FTC. Refer to the FTC's website at [www.identitytheft.gov](http://www.identitytheft.gov) for additional information, protection strategies, and resources.

**Privacy Act and Paperwork Reduction Notice**

Our legal authority to request the information is 26 U.S.C. 6001.  
The primary purpose of the form is to provide a method of reporting identity theft issues to the IRS so that the IRS may document situations where individuals are or may be victims of identity theft. Additional purposes include the use in the determination of proper tax liability and to relieve taxpayer burden. The information may be disclosed only as provided by 26 U.S.C. 6103. Providing the information on this form is voluntary. However, if you do not provide the information it may be more difficult to assist you in resolving your identity theft issue. If you are a potential victim of identity theft and do not provide the required substantiation information, we may not be able to place a marker on your account to assist with future protection. If you are a victim of identity theft and do not provide the required information, it may be difficult for IRS to determine your correct tax liability. If you intentionally provide false information, you may be subject to criminal penalties.  
You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by section 6103.  
Public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. If you have comments concerning the accuracy of these time estimates or suggestions for making this form simpler, we would be happy to hear from you. You can write to the Internal Revenue Service, Tax Products Coordinating Committee, SE:W-CAR:MP:T:T:SP, 1111 Constitution Ave. NW, IR-6526, Washington, DC 20224. Do not send this form to this address. Instead, see the form for filing instructions. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

# Identity Theft Affidavit

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers)

- ☐ I am submitting this form in response to a mailed notice or letter from the IRS.
- ☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & D.

**Note to all filers:** Failure to provide required information on **BOTH** sides of this form **AND** clear and legible documentation will delay processing.

## THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).

### Section A - Reason For Filing This Form (Required for all filers)

Check only **ONE** of the following two boxes. You **MUST** provide the requested description or explanation in the lined area below.

- 1 ☐ I am a victim of identity theft **AND** it is affecting my federal tax records.

*You should check this box if, for example, your attempt to file electronically was rejected because someone had already filed using your Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN), or if you received a notice or correspondence from the IRS indicating someone was otherwise using your number.*

Provide a short explanation of the problem and how you were made aware of it.

- 2 ☐ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

*You should check this box if you are the victim of non-federal tax related identity theft, such as the misuse of your personal identity information to obtain credit. You should also check this box if no identity theft violation has occurred, but you have experienced an event that could result in identity theft, such as a lost/stolen purse or wallet, home robbery, etc.*

Briefly describe the identity theft violation(s) and/or the event(s) of concern. Include the date(s) of the incident(s).

### Section B - Taxpayer Information (Required for all filers)

Taxpayer's last name	First name	Middle initial	The last 4 digits of the taxpayer's SSN or the taxpayer's complete Individual Taxpayer Identification Number (ITIN)
----------------------	------------	----------------	---

Taxpayer's **current** mailing address (apt., suite no. and street, or P.O. Box)

City	State	ZIP code
------	-------	----------

Tax year(s) affected (Required if you checked box 1 in Section A above)	Last tax return filed (year) (If you are not required to file a return, enter NRF and do not complete the next two lines)
---	---

Address on last tax return filed (If same as current address, write "same as above")

City (on last tax return filed)	State	ZIP code
---------------------------------	-------	----------

### Section C - Telephone Contact Information (Required for all filers)

Telephone number (include area code) <input type="checkbox"/> Home <input type="checkbox"/> Work <input type="checkbox"/> Cell	Best time(s) to call
--	----------------------

I prefer to be contacted in (select the appropriate language) ☐ English ☐ Spanish ☐ Other \_\_\_\_\_

### Section D - Required Documentation (Required for all filers)

Submit this completed form and a **clear and legible** photocopy of at least one of the following documents to verify your identity. If you are submitting this form on behalf of another person, the documentation should be for that person. If necessary, enlarge the photocopies so all information and pictures are clearly visible.

Check the box next to the document(s) you are submitting:

- ☐ Passport ☐ Driver's license ☐ Social Security Card ☐ Other valid U.S. Federal or State government issued identification\*\*

\*\* Do not submit photocopies of federally issued identification where prohibited by 18 U.S.C. 701 (e.g., official badges designating federal employment).



# Internet Crime Complaint Center



## Data, Tools, and Resources for Enforcement Professionals

The Internet Crime Complaint Center (IC3) is an alliance between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI).

IC3's mission is to address crime committed over the Internet. For victims of Internet crime, IC3 provides a convenient and easy way to alert authorities of a suspected violation. For law enforcement and regulatory agencies, IC3 offers a central repository for complaints related to Internet crime, uses the information to quantify patterns, and provides timely statistical data of current trends.

### Features

- Provides a central point for Internet crime victims to report and to alert an appropriate agency on-line at [www.ic3.gov](http://www.ic3.gov)
- Collects, reviews, and refers Internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts
- Identifies current crime trends over the Internet

### Benefits

- Provides an analytical repository for Internet crime complaints
- Analyzes and refers all fraudulent activity identified on the Internet to the appropriate local, state, or federal law enforcement authority
- Aids in the development of law enforcement training to address identified Internet crime problems
- Serves as the catalyst that allows law enforcement and regulatory agencies to network and share data
- Potentially reduces the amount of economic loss by Internet crime throughout the United States

**To file an Internet crime  
complaint, visit the IC3  
Web site at [www.ic3.gov](http://www.ic3.gov).**

