

What to do if you are a victim of identity theft?

If you do become a victim of identity theft, there are four steps that must be taken immediately in order to minimize the damage done by the thieves. It is also critical that you keep a record with the details of your conversations and copies of all correspondence.

1. Place a fraud alert on your credit reports and review your credit reports.

Fraud alerts act to prevent identity thieves from opening new accounts in your name. To place such an alert on your credit report you need to contact one of the three consumer reporting agencies listed below. Whichever consumer reporting agency you contact will notify the other two accordingly. Once you have placed the fraud alert on your account you are entitled to a free credit report. Scrutinize this document carefully, note any inaccurate information, contact the issuing consumer reporting agency and have it removed immediately.

Equifax, (800) 525-6285, www.equifax.com, P.O. Box 740241, Atlanta, GA 30374-0241

Experian, (888) 397-3742, www.experian.com, P.O. Box 9532, Allen, TX 75013

TransUnion, (800) 680-7289, www.transunion.com, Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

2. Close accounts that you know, or believe, have been tampered with or opened fraudulently.

It is imperative that you contact each company directly and notify them in writing that you believe your account has either been accessed, or opened illegally. Ask each company specifically what their governing identify theft reporting procedures are so that you can properly dispute the charges. Also be sure to provide copies of supporting documents to these companies (i.e. police reports, bank statements, etc), but retain the originals for your own records. In addition, send all correspondence via certified mail, with a return receipt requested, in order to catalog your correspondence with the various companies. Lastly, once you have resolved the dispute with the respective companies, ask that them to provide you with a letter that confirms the resolution and discharges the fraudulent debts.

3. File a report with your local police or the police in the community where the identity theft took place.

Often companies require that you provide them with some evidence of the crime in order to discharge the fraudulent charges, so if you cannot obtain a copy of the police report, at least note the report number, the responding officer and that officer's department. You should also contact the state Attorney General to inquire if there are any applicable state requirements for reporting identity theft.

The contact information for the Honolulu Police Department (HPD) and the Hawaii Attorney General's office is listed subsequently.

What to do if you are a victim of identity theft?

4. File a complaint with the FTC.

Reporting the theft of your identity to the FTC assists local law enforcement agencies to better track and ultimately capture these identity thieves. The FTC can also refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

The FTC is the single best source of information on identity theft. All the statistical data and recommendations exposed in this article are drawn directly from either FTC publications, or the FTC identity theft website at <http://www.consumer.gov/idtheft>. Those without Internet access can contact the FTC directly at (877) 438-4338, Identity Theft Clearinghouse, FTC, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Ways to protect against identity theft

The best way to avoid becoming an identity theft victim is to exercise caution, prudence and diligence in protecting your sensitive personal information.

1. Set up passwords on your credit card, bank, phone and computer accounts. Avoid using easily identifiable passwords like your SSN, birthdate, or mother's maiden name. Change the passwords at fluctuating intervals.
2. Secure personal information inside your home in some type of safe or lock box, especially if you have roommates or employ outside contractors who have access to your home.
3. Inquire of your employer as to the location of where your personal information is kept and what the governing procedures are regarding the release of that information.
4. Avoid giving personal information out via either the phone, Internet or regular mail unless you have positively identified the other party with whom you are dealing.
5. Deposit your outgoing mail in secure U.S. Postal mailboxes, as opposed to the personal mailbox at your residence. If you must utilize your personal mailbox to send outgoing mail, do not highlight that the receptacle contains such information by raising the flag or comparable indicator. Check your mailbox for incoming correspondence daily and if you are going to be away from home for an extended period call the U.S. Postal Service at (877) 275-8777 to ask for a vacation hold.
6. Keep your SSN card in a secure location and only reveal your number when absolutely necessary. Ask to use other types of identifiers if possible. If your state uses your SSN as your driver's license number, ask to substitute another number.
7. Only carry on your person the identification information and financial cards that you absolutely need.
8. Keep your purse or wallet in a safe place both at home and in your place of employment.
9. Pay attention to your billing cycles. Not receiving a regularly scheduled monthly bill in the mail is a good indicator that your identity has been, or is about to be, stolen. Contact your creditors anytime your bills do not arrive on time.
10. Be extraordinary thorough in safeguarding any computer that contains your sensitive personal information, whether that unit is in your home or at work. Update your virus protection regularly. Avoid downloading any file from individuals whom you do not know. Use a firewall to limit the amount of access thieves have to your computer. Use a secure browser to guard the safety of your online transactions. Avoid keeping financial information on your computer unless absolutely necessary. Do not use any automatic log in features that would allow a thief to easily defeat the password security precautions. Delete all sensitive personal information from your computer before you dispose of it.