

## You have fraud – Now what?

What should you do if your information is lost or stolen but your accounts do not show or indicate any problems?

If your wallet, social security card, other personal financial or account information is lost or stolen; contact the credit reporting agencies and place a fraud alert on your credit file. Check all bank and other account statements for any potential unusual activity. Depending on the information that was lost/stolen, you may want to take additional steps, such as, requesting a free copy of your credit report from [annualcreditreport.com](http://annualcreditreport.com), change passwords on all accounts and email, etc.



### **Immediate steps to be taken once identity theft has been discovered.**

1. Place an initial fraud alert on your credit file/report.
2. Order a copy of your credit reports (Trans Union, Experian and Equifax). *See the checklist on page 2.*
3. Create and identity theft report.
4. File a police report.



### **Create a system to organize your papers, record contacts/correspondence and track deadlines.**

1. Track all calls made to creditors and law enforcement.
2. Create a log of all telephone calls.
3. Record the date of each call along with the names and telephone numbers of everyone you contacted.
4. Prepare your questions before you call and write the answers provided to you.
5. Send all correspondence via certified mail with a return receipt.
6. Create a filing system.
7. Keep all originals.
8. Send copies of your documents and reports, do NOT send originals.
9. Make a timeline.
10. List dates by which you must file your requests.
11. List dates by which a company/creditor must respond to you.
12. List dates by which you must send follow-up.

**+ Fraud Checklist** *(If applicable)*

- Place a fraud alert on your credit report. This is free and remains on your credit file for 90-days.
- There are 3-major credit reporting agencies Trans Union, Equifax and Experian. You can place an alert on all 3 simply by contacting just one of them. You contact them as follows: Trans Union-800.680.7289, Equifax-800.525.6285 and Experian-888.397.3742; websites [www.transunion.com](http://www.transunion.com), [www.equifax.com](http://www.equifax.com) or [www.experian.com](http://www.experian.com).
- Consider placing a “Freeze” on your credit report. This is different from an Alert, “Freeze” can stay on for up to 7-years.
- File a police report.
- Notify the FTC at 877.ID THEFT or visit their website at [www.ftc.gov](http://www.ftc.gov) (Best ID Theft website; there is a comprehensive step by step process and instructions on how to get a recovery plan started.).
- Add a password or passcode to all your bank accounts.
- Change your compromised account numbers by closing those accounts and opening new ones.
- Change your password with your email provider.
- Notify all lenders, credit card companies and any financial institutions that you have any account with so that they can add security alerts to all of your accounts.
- Going forward monitor your credit report diligently. You can get an annual free credit report at [www.annualcreditreport.com](http://www.annualcreditreport.com).
- Report your ID Theft to State and Federal Agencies.
- Notify the U.S. Social Security Administration at [www.ssa.gov](http://www.ssa.gov) or 800.269.0271.
- If personal checks have been lost/stolen, contact ChexSystems to report the stolen checks at 800.428.9623 or by writing them at ChexSystems, Attention: Consumer Relations, 7805 Hudson Road, Suite 100, Woodbury, MN 55125.
- Contact the IRS’s ID Protection specialized unit at 800.908.4490 so that precautions can be used when you file your tax returns.
- Opt out of pre-screen offers at 888.567.8688 or visit [www.optoutprescreen.com](http://www.optoutprescreen.com).
- If your driver’s license number has been stolen or compromised, contact the Department of Motor Vehicles.