

IDENTITY THEFT PROTECTION CHECKLIST

Identity theft is a risk that continues to grow and change daily. Due to the many forms identity theft can take, including medical, credit and financial theft, the threat remains prevalent and affects millions of people per year.

Keeping up-to-date with the latest prevention methods is the surest way to protect your assets and identity. Here are a number of steps you can take to reduce the risk of identity theft happening to you. We have also included steps to take if you are unfortunate enough to suffer this loss.

1. Reduce access to your personal information – if asked for your Social Security number, be sure to inquire why it is needed and then how it will be protected.

- If you are applying for a credit card or insurance, you will typically be required to provide your Social Security number so the provider can pull your credit report.
- When asked for this information by your doctor's office, you should insist that the information on your insurance card is sufficient.
- Do not provide your Social Security number to online job websites or over the phone to strangers.

2. Eliminate unwanted credit solicitations – reduce the chance of fraud perpetrated on you by removing unwanted solicitations. Take the following preventative steps:

- Contact 888.567.8688 and opt out of pre-screened credit applications or go to www.optoutprescreen.com.
- Register for the National Do Not Call Registry that gives you a choice whether to receive telemarketing calls at home. Go to www.donotcall.gov/register/reg.aspx to fill out the form and submit.
- Contact DMA Opt-Out Preference Service to limit direct marketing efforts.
- Ask your credit card companies to cease sending convenience checks.

3. Do not respond to emails requesting personal information – “phishing” is a technique used by criminals to solicit your personal data by sending what appears to be a legitimate email request from a recognized source, including banks, credit card companies or social networking sites.

- Be suspicious of any email that asks for sensitive personal information, even if the sender is familiar to you.
- Avoid filling out forms contained in an email message or pop-ups, even if it appears to be from a company that you do business with.
- If you receive an email from what appears to be your bank or credit card company, call them to confirm – and use the telephone number on your bank or credit statement, NOT the one in the “phishing” email. Emails with misspellings or poor grammar are usually a good indication the sender is a fraud.

4. Buy a shredder that cuts your paper into confetti – thieves use discarded information to collect personal data on victims. A paper shredder reduces the potential for “dumpster diving” thieves to obtain your personal data from the following sources:

- Credit applications
- Expired credit cards
- Old bank and credit card statements
- Renewal forms that contain personal data
- Unwanted and unused convenience checks

5. Keep track of insurance cards – guard your insurance card as you would your credit or ATM cards.

- Never give your medical information over the phone or lend your card to a friend.
- Medicare recipients need to be extremely careful as their Social Security numbers are printed on their Medicare cards.

6. Monitor your financial records – review your credit card and bank statements each month. Refute any unauthorized charges within 30-60 days. Call your bank or credit card company immediately if you see any activity that could be fraudulent.

- Use passwords that are not easily guessed.
- Do not share passwords with anyone.
- Purchase virus, adware and firewall protection for your internal access.
- If you have a wireless network, make certain that access is encrypted.
- Warn your children of the dangers of the Internet, including stalking, spyware, viruses and other potential threats.

7. Monitor your medical statements – *every time you receive an explanation of benefits (EOB) form from your health insurance company, check it carefully.*

- If you see charges for treatments you don't recall receiving, contact your insurance company for more information.
- Ask your insurer to provide you an annual summary of claims submitted under your name. Thieves may redirect your EOBs to a fake address, making it more difficult for you to identify a breach.

8. Monitor your medical records – *request a copy of your medical records from your physician(s) and keep in a secure place.*

- If your medical identity is stolen and your medical records are altered, you'll have documentation to prove who you are when you report the fraud. It will also make it easier for you to prove the fraud and correct your medical records.

9. Review Social Security benefits

- Review your Social Security statement to identify attempts to use your identity to seek employment.
- Contact 800.772.1213 to request an earnings and benefit statement or request the information via the Internet at www.ssa.gov.

10. Check your credit report regularly

- You can get a free annual copy of your report from all three credit reporting agencies at www.annualcreditreport.com.

This information was provided by HUB International Personal Insurance. It is provided for general information purposes only and does not constitute professional advice.

STEPS TO TAKE IF IDENTITY THEFT OCCURS

1. Report the fraud to the three major credit bureaus – fraud departments for the three bureaus can be contacted at:

Experian

POB 9532
Allen, TX 75013
888.397.3742

Equifax

POB 740241
Atlanta, GA 30374
888.766.0008

**TransUnion – Fraud
Victims Asst. Dept.**

POB 6790
Fullerton, CA 92634
800.680.7289

Ask them to flag your accounts with “fraud alerts” requiring notice to you prior to opening any new account.

2. Contact all of your creditors

- Notify credit card companies, utility service, telephone and Internet providers that you have been a victim of fraud.
- Stop payment on outstanding checks and report the fraud to check verification companies:
 - National Check Fraud 843.571.2143
 - Telecheck 800.710.9898
- Close all accounts that have been compromised.
- Close and reopen checking and savings accounts.

3. Notify the police

- If the local police refuse to take a report, advise them you need it for insurance purposes.

4. File a claim with the Federal Trade Commission

- Call 877.ID.THEFT

5. Contact your health insurance company if you think your medical identity has been compromised.

- Insurance policies offer some relief from the cost of professional assistance in re-establishing your own credit and identity.

This information was provided by HUB International Personal Insurance. It is provided for general information purposes only and does not constitute professional advice.