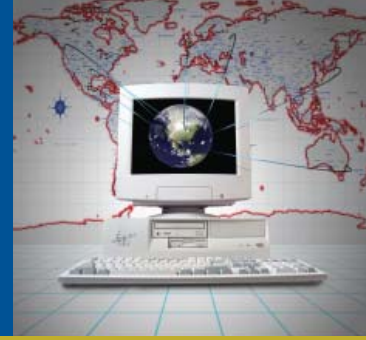


Identity Theft and Cyber Security Check List

HUB International Personal Insurance



With over ten million individuals experiencing some form of identity theft last year, prevention is more important than ever. Countless examples of breaches of corporate security have given rise to more and more concern about protecting our personal information. Stolen lap tops, compromised firewalls and missing data tapes have placed the personal financial records of countless victims in the hands of identity thieves.

Insurance policies may offer some relief from the cost of professional assistance in re-establishing your own credit and identity. However, there is no coverage or solution for recovering the time needed to reverse the damage. The Federal Trade Commission estimates that the average victim of identity theft will expend over 600 hours to clear his or her name. The estimated time for full recovery is 14 to 16 months.

The “soft” costs associated with recovering one’s identity are not transferable. Consequently, the best advice is to create a plan that mitigates the potential for a loss to occur. 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. Buy a shredder that cuts your paper into confetti

Thieves use discarded information to collect personal data on victims. A confetti shredder should be used on any material that contains personal data:

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

□ 2. Eliminate unwanted credit solicitations

Reduce the chance of fraud perpetrated on you by removing unwanted solicitations. Take the following preventive steps:

- Contact 888-567-8688 and opt out of pre-screened credit card applications.
- Register for the national do not call list
- Contact DMA Opt-Out Preference Service to limit direct marketing efforts www.dmaconsumers.org/privacy.html
- Ask your credit card companies to cease sending convenience checks

❑ 3. Reduce access to your personal data

In addition to “dumpster diving” thieves employ a number of methods to secure personal data. Guard your information carefully both in and outside your home:

- Watch for “shoulder surfing” at ATM machines. Change locations if you are suspicious of the surroundings.
- Do not give personal information via email or telephone unless you have initiated the contact. “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 credit source.
 - ❑ Fraudulent emails will not permit access to the credit source home web site.
 - ❑ There are often misspellings or poor grammar in the content of the email.
 - ❑ Contact the telephone number on your credit card, NOT the one in the “phishing” email.
- Do not carry your social security card with you. Refuse to provide this information without a proper explanation for its use.
- Stop mail delivery when you are away from home to prevent a build up that ID thieves can remove.

❑ 4. Monitor your financial records

Credit card and bank statements should be reviewed each month. Charges that you cannot identify should be investigated.

- Secure cancelled checks and bank statements in a location with limited or protected access.
- Keep a record of all open accounts in the event you need to rebuild your ID. Store these records in a safe place.

❑ 5. Review Social Security Benefits

Review your annual Social Security benefits report for accuracy. Alert the Social Security Administration of any irregularities.

- Review of your social security statement can highlight attempts to seek employment using your identity.
- Contact 800-772-1213 to request earnings and benefit statement.
- You may request the information via the internet www.ssa.gov

❑ 6. Lock out thieves from entering via a cyber portal

Access to the internet and personal computers should be treated like your front door.

- Use passwords that are not easily guessed.
- Do not share passwords with anyone.
- Purchase virus, adware and firewall protection for your internet 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. Be prepared to protect yourself if ID theft occurs

Copies of your financial records could prove invaluable in the event of an occurrence.

- Organize your records and keep copies of all agreements, contact information and account information.
- Have contact information for the three credit bureaus available for immediate notice.

□ 8. Find out what insurance protection exists

If you are not sure what coverage you have for this type of a loss, contact your provider and request an update.

- Insurance can mitigate some of the expenses related to restore your identity.
- The soft cost surrounding this issue such as lost time for the victim are immeasurable and in general not insurable.
- Prevention of a theft of your identity, while not perfect, is the best treatment method in the current market conditions.

Steps to take if ID theft occurs

□ 1. Report the fraud to the three major credit bureaus

Fraud department for the three bureaus can be contacted at:

- | | | |
|---|---|---|
| <ul style="list-style-type: none"> ■ Experian
POB 9532
Allen TX 75013
888-397-3742 | <ul style="list-style-type: none"> ■ Equifax
Fraud Assistance
POB 105068
Atlanta GA 303348-5069
888-766-0008 | <ul style="list-style-type: none"> ■ TransUnion
Fraud Victims Assistance Department
POB 6790
Fullerton CA 92634
800-680-7289 |
|---|---|---|

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 that you need it for insurance purposes
 - Notify your local postal inspector and report this as a crime
- **4. File a claim with the Federal Trade Commission**
 - Contact for the FTC is 877-ID THEFT
- **5. File a claim under your homeowners insurance**
 - Not all carriers offer this coverage. Some provide the protection or increased protection by endorsement for additional premium.
 - Coverage will vary but typically offers reimbursement for unwarranted charges and the fees associated with professionals need to re-establish your identity.
 - Keep records of all charges and professional fees incurred as a result of the loss
 - Keep in mind a significant part of the loss is uninsured. The loss of time needed to repair your identity cannot be insured or replaced. Practice prevention to reduce the risk of this unpleasant experience.

HUB International is a leading national property casualty firm with over 200 offices throughout the U.S. and Canada. Our specialists understand and can provide solutions to a broad range of coverage needs for homes, automobiles, valuable possessions, personal liability or specialty products such as yachts, equine, aircraft and other interests.

Contact you HUB International Personal Insurance specialist today.