Identity theft insurance

Steps and advice to help protect you from identity predators

Other Insurance Topics

IN THIS ARTICLE

SHARE THIS

- EN ESPAÃ‘OL
- DOWNLOAD TO PDF

Identity theft victims often spend months or years recovering from the frauds perpetrated on their bank accounts and getting their credit rating corrected. Protect yourself against identity theft with this advice.

What is identity theft?

Identity theft is the act of taking personal informationâ€”like Social Security numbers or bank account numbersâ€”and using it to "impersonate" someone for the purpose of stealing.

These crimes are usually financial in nature. For example, identity thieves typically:

- Use stolen credit card numbers
- Take money from victims' bank accounts
- Open unauthorized credit cards
- Obtain unauthorized bank loans

In some more elaborate schemes, criminals even use the stolen personal information to get a job, take out an insurance policy, rent a home or take out a mortgage in the victimâ€™s name.

How do the identity thieves steal information?

- **By stealing or otherwise obtaining physical documents** â€“ Many identity theft cases are the result of a lost or stolen wallet, checkbook, credit card or other physical document. Some store credit cards may still require Social Security numbers or other credit information on their written applicationsâ€”there have been instances of these applications being stolen and used by identity thieves. More intrepid thieves use old-fashioned methods, such as â€˜dumpster divingâ€™â€”that is, rooting around in peopleâ€™s garbage to collect financial information.

- **By stealing or obtaining hardware** â€“ Your laptop, thumb drives and other electronic data storage devices are a rich source of your personal information.

- **By coaxing personal information via phone calls** â€“ Unless you yourself have initiated the phonecall, do not give any private data to callers. Legitimate financial institutions and businesses make it a point to keep information secure and will not ask to you provide it over the phone.

- **By obtaining personal information via online means** â€“ Some identity theft schemes use online scams like â€˜phishingâ€™â€”where thieves use email inquiries purporting to be from financial or other online organizations to obtain sensitive account information. Identity theft is a potential problem when computer servers at large institutions are hacked and breached and with online shopping or other websites that don't have security safeguards in place.

What is the impact of identity theft?

Victims of identity theft fraud often travel a long and frustrating road to recovery. Depending on the severity of the identity theft fraud damage, the recovery process (including getting credit records corrected) can take anywhere from a few weeks to several years. In the meantime, victims are often left with lower credit scores and may have difficulty getting credit, obtaining loans and even finding employment.

Does insurance cover identity theft?

With most credit cards, once you've reported the card missing, you're only liable for a stated amount of the fraudulent charges. Homeowners insurance and renters policies may provide a limited amount protection for loss of cash or credit cards.

However, identity theft comes with not only financial loss, but far reaching consequences like blows to your credit and reputation that may take much time and paid professional expertise to resolve. As a result, many companies now provide insurance products that not only cover costs associated with identity theft incident recovery, but also provide "restoration" services to make the process easier and faster.

Policies vary by insurer and by state, but some of coverages and services that may be provided include:

- Assignment of a consumer fraud specialist or case manager
- Replacement of government issue identifications
- Assisting with civil judgments, criminal charges, audits or hearings related to fraud perpetrated by the "impostor"
- Resolution services to help reclaim identity and restore credit
- Reimbursement of attorney's fees
- Reimbursement of administrative fees and expenses and fees

Tips for avoiding identity theft

- **Keep the amount of personal information in your purse or wallet to the bare minimum.** Avoid carrying additional credit cards, your social security card or passport unless absolutely necessary.

- **Guard your credit card when making purchases.** Be vigilant about good credit card keeping habitsâ€”for example, make it a point to keep your wallet in your hand until the clerk gives back your card. Donâ€™t fall prey to â€œshoulder surfersâ€• who may be nearbyâ€”shield your hand when using ATM machines and be alert to those around you when giving out personal information on the phone.

- **Always take credit card or ATM receipts.** Donâ€™t throw them into public trash containers, leave them on the counter or put them in your shopping bag where they can easily fall out or get stolen.

- **Do not give out personal information.** Whether on the phone, through the mail or over the Internet, donâ€™t give out any personal information unless you have initiated the contact, are sure you know who you are dealing with and that the line is secure.

- **Proceed with caution when shopping online.** Use only secure, authenticated websites to conduct business online. Before submitting personal or financial information through a website, check for the locked padlock image on your browserâ€™s status bar or look for "https://" (rather than http://) in your browser windowâ€”the "s" indicates a higher level of security. If you have any concerns about the authenticity of a web page, contact the owner of the site to confirm the URL.

- **Be aware of phishing and pharming scams.** In these scams, criminals use fake emails and websites to impersonate legitimate organizations. Exercise caution when opening emails, attachments and instant messages from unknown sources. *Never* give out personal, financial or password related information via email.

- **Make sure your computer security is up to date.** Have firewall, anti-spyware and anti-virus programs installed on your computer and update regularly.

- **Monitor your accounts.** Donâ€™t just rely on your credit card company or bank to alert you of suspicious activity. Carefully monitor your bank and credit card statements to make sure all transactions are accurate. If you suspect a problem, contact your credit card company or bank immediately.

- **Order copies of your credit report and review for errors.** Preferably, get one from each of the three major credit reporting bureaus (Equifax, Experian). By law, you should be able to get at least one for free, and many banks and other financial institutions provide them as a service to their customers.

Your credit report contains information on where you work and live, the credit accounts that have been opened in your name, how you pay your bills and whether you've been sued, arrested or filed for bankruptcy. Make sure these reports accurate and includes only those activities you've authorized.

- **Place fraud alerts at the major credit bureaus.** A fraud alert at tells creditors to contact you before opening any new accounts or before making any changes (like changes of address) to your existing accounts. This makes it more difficult for identity thieves to open accounts in your name. Â You just have to contact one bureau; by law, the agency you contact is required to contact the other two.

- **Use secure passwords on your credit card, bank and phone accounts.** Avoid using easily available information like your mother's maiden name, your birth date, any part of your Social Security number or phone number, or any series of consecutive numbers. If you suspect a problem with your credit card, change your password.

- **Shred documents with personal information before disposing of them.** This includes any paperwork with credit card numbers, bank statements, charge receipts or credit card applications.

What to do if you're an identity theft victim

- **If you've had a theft where your personal information has been compromised**, such as stolen wallet or credit cards or a phishing scam, immediately report it to the credit card company, applicable financial institutions, and to the police. Ask for a copy of the police report (you will need it if you want to file an insurance claim).

- **If you areâ€”or suspect you've beenâ€”the victim of a phishing scam or other electronic incident** , immediately report the incident to any of your financial institutions or credit card companies that might be compromised, and register a fraud alert with a credit reporting company.

- **Learn more about potential large scale data breaches and privacy issues** from organizations such as the non-profit Privacy Rights Clearing House.

- **Report identity theft incidents or attempts to federal agencies** that monitor them, such as the FBI Internet Crime Complaint Center and the Federal Trade Commission (FTC) Consumer Information Identity Theft, which can provide further advice and assistance.

Additional resources

Major credit bureaus:

- Equifax
- TransUnion
- Experian

Federal Bureau of Investigation (FBI) Internet Crime Complaint Center

Federal Trade Commission (FTC) Consumer Information for Identity Theft

- Online FTC Identity Theft
- Or call 877-IDTHEFT

Privacy Rights Clearing House

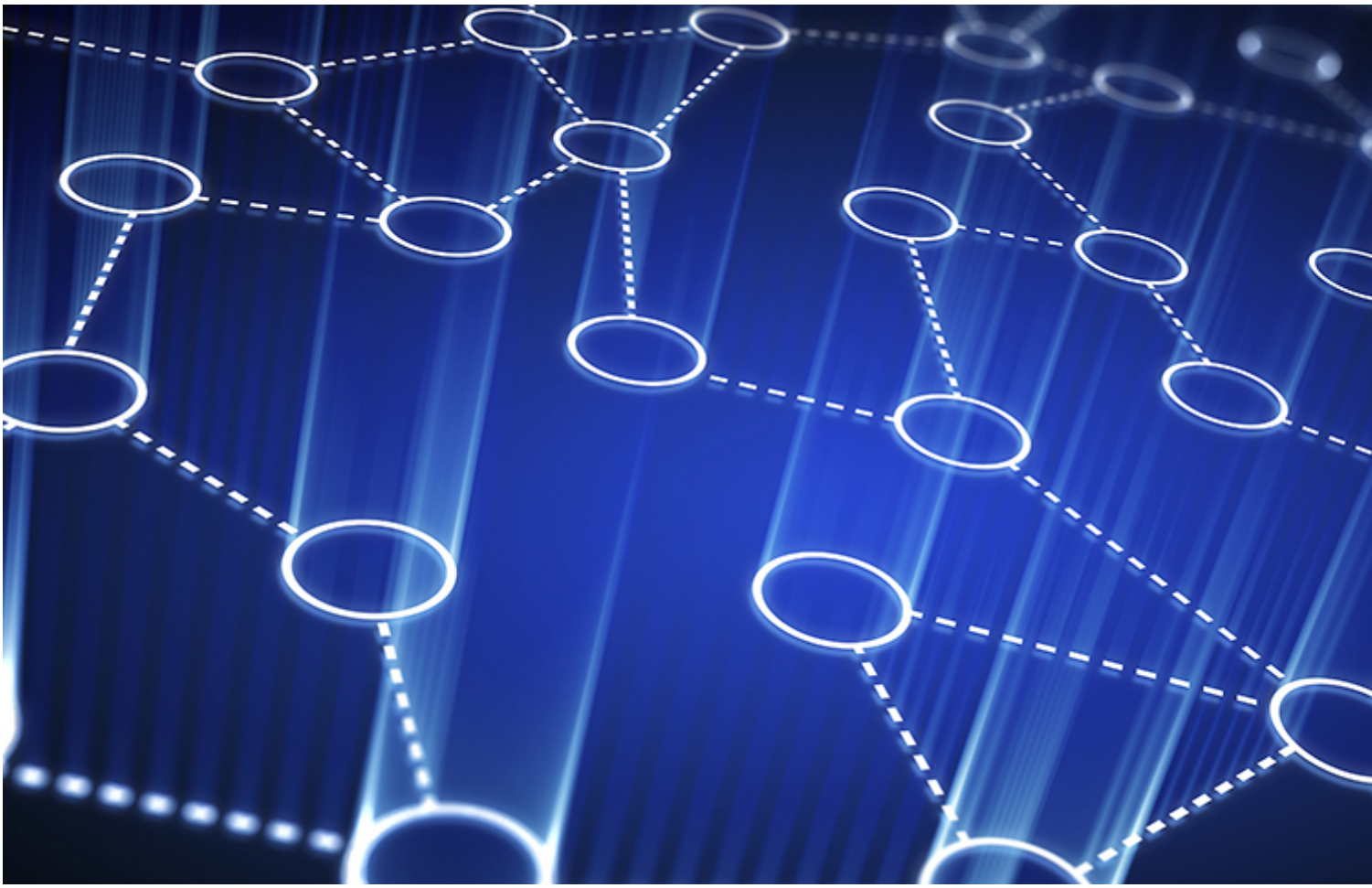
The U.S. Department of Justice - Identity Theft and Identity Fraud

Â

Next steps link: Protect your belongings as well as your identity by securing your home against burglary.

Back to top

You May Also Like



Business Insurance
Cyber liability risks