

# IDENTITY THEFT IS ON THE RISE

**I**dentify theft has grown exponentially over the past few years, spurred by the financial rewards, the relative ease of committing the crime, and the low probability of being caught. According to the Federal Trade Commission, nearly 15 million Americans are victimized each year, costing consumers \$5 billion, and banks and corporations \$56 billion every year. To clean up one's credit report and associated complications requires an average of \$1173 and 175 hours.

Stealing wallets or purses was once the primary method to obtain another person's personal information. Today, "dumpster diving," combined with Internet Web sites and search engines, help criminals identify and exploit their victims.

Criminals gain access to individuals' credit reports by posing as potential landlords, employers or loan officers. They "shoulder surf" at checkout lines and videotape transactions at ATM machines to capture PIN numbers. They steal mail from mailboxes for bank or credit card statements and newly issued credit cards, and "dumpster dive" in trash bins for credit card and loan applications that have not been shredded. After combining key pieces of individuals' identities, they are able to impersonate their victims, obtain loans and steal the money.

Identity thieves are very brazen. In one incident, the identity thief took out a life insurance policy on his victim. In another incident, an identity thief was arrested after two victims living in the same apartment complex struck up a conversation about their travails. This coincidental conversation ultimately led the police to arrest a person that worked in the business office of the complex and had access to the rental applications and credit reports of present and past tenants.

Contrary to popular belief, even people with bad credit can be victims of identity theft.

Generally, victims of banking and credit card fraud will be liable for no more than the first \$50 of the loss. However, the victim must notify financial institutions within two days of learning of the loss to avoid being responsible for the fraudulent activity.

Even though victims are usually not responsible for paying their imposters' bills, their credit report is always left in shambles.

It takes months or even years to regain their financial health. In the meantime, they have difficulty writing checks, obtaining loans and housing, and even getting a job. Victims of identity theft seldom find help from the legal authorities as they untangle the web of deception created by their imposter.



## RECOMMENDATIONS

Consider these recommendations to reduce your potential risk of identity theft:

### Social Security Number

1. Guard your Social Security number vigilantly. It is the key to your credit report and is the criminals' prime target.

2. Do not print your SSN on your checks.

3. Order your Social Security Earnings and Benefits Statement once a year and look for employers you didn't work for. Someone may be using your identity for a job.

4. Monitor your credit report. It contains your SSN, present and past employers, a listing of all account numbers, including those that have been closed, and your credit score. After applying for a loan, credit card, rental, or anything else that requires a credit report, request that your SSN on the application be truncated or completely obliterated, and your original credit report be shredded once a decision has been made. (A lender or rental manager needs to retain only your name and credit score to justify his/her decision.)

### Internet / Computers

5. Make sure your computer is protected with Internet security software that is updated regularly. **See Cyber Crime, Page 16.**

6. Do not download anything from the Internet that you did not solicit. Activate the pop-up blocker on your computer.

7. Shop only on secure websites. The web address should begin with https://. It must have the "s" or it is not a secure site. You can also look for a padlock or key in the bottom right corner of your screen.

8. Avoid using a debit card when shopping online. Credit cards have a maximum liability of \$50 for fraudulent charges; debit cards can go up to \$500 or more.

9. Use a real password. While it is easier for you to have one that is simple, it is also easier for crooks.

10. When possible, choose to have a second-level password on an account. Choose a password that is more difficult than your mother's maiden name.

11. Never leave your laptop anywhere you wouldn't leave your baby...in the car, in a gym bag, at a restaurant. According to

Amitron.org, stolen laptops and computers account for nearly 40% of security breaches.

12. Before donating your computer to a recycling center, completely wipe out all confidential information. This requires special software, and more than just reformatting.

### Credit Cards

13. Shred old bank and credit card statements, "junk mail" credit card offers and old tax returns. Use a crosscut shredder. Crosscut shredders cost more than regular shredders but are superior. When Iranian students in Tehran stormed the US embassy in 1979, the embassy staff had shredded their most important documents; however, they used a regular shredder. The enterprising students hired carpet weavers and reconstructed the shredded documents.

14. Never give your credit card number or personal information over the phone unless you initiated the call and trust that company.

15. When you are shopping or dining, be aware of how salespeople or waiters handle your card. Make sure they do not have a chance to copy your card.

16. Examine the charges on your credit card when your statement arrives. Also, keep track of the billing cycles of your cards. If a statement doesn't arrive when it should, it could mean that a thief has changed the mailing address on your account.

17. Minimize the number of credit cards you own to reduce the opportunity for a

criminal to steal a card.

18. Carry extra credit cards or other identity documents only when needed.

19. Shred the card on unused credit card accounts. If you close the account, it may lower your credit score because of reduced credit availability.

20. Put a fraud alert tag on your credit report, which will limit a thief's ability to open accounts in your name.

### **Checks**

21. Use high security checks like those shown on **Pages 10 – 11**. Criminals "wash" ordinary checks in chemicals, dissolving what you wrote without leaving evidence. After the check is dry, forgers insert new data. High security checks react to chemicals, showing that they have been washed.

22. Do not mail checks from home. They can be stolen from your mailbox, chemically washed and re-used. Go to the post office.

23. When writing manual checks, use the uni-ball® 207 gel pen. Its ink will not dissolve in chemicals.

### **Miscellaneous**

24. Be highly suspicious of unsolicited emails or letters that say you won money.

25. Remove your name from the marketing lists of the three credit reporting bureaus to reduce pre-approved credit offers.

26. Add your name to the Name Deletion List of the Direct Marketing Association ([www.dmchoice/consumerassistance.php](http://www.dmchoice/consumerassistance.php)).

27. Subscribe to Privacy Guard or another similar service to alert you if your credit history is being requested.

28. Avoid ATMs that are not connected to a bank or a reputable business. Shield the keypad when entering your PIN.

29. Protect your incoming mail by picking it up ASAP. If you will be away for a period of

time, have your mail held at the post office.

30. Keep your purse or wallet in a locked drawer at work. Find out how the company protects your personal information, and who has access to your direct deposit information.

31. Photocopy and retain the contents of your wallet. Copy both sides of each license and credit card so you have the account numbers, expiration dates and phone numbers if your wallet or purse is stolen.

32. Keep Social Security cards, birth certificates and passports in a locked box.

33. Read the privacy policies of the companies with whom you do business. Opt out of having your information shared.

34. Protect a dead relative. Contact the credit bureaus and put a "deceased" alert on the person's reports. Send copies of the death certificate to institutions where the person had an account.

## **SOMETHING FOR NOTHING**

"There's no such thing as a free lunch." If something seems too good to be true, it isn't. Thousands of people have been burned by the "lottery" scam, which works like this: The "target" is emailed that he/she has won a prize, and that the first check will be sent soon. Follow up emails explain that taxes must be pre-paid on the winnings, but a partial payment greater than the taxes owed is being sent. The person is instructed to deposit the check, wire transfer payment for the taxes, and keep the balance. Final payment is promised upon receipt of the taxes. Of course, the first check is bogus and is returned unpaid and charged back to the person's account. The person is liable to his/her bank for the check's face value, most of which is gone. This scam has many variations, but they all offer something for nothing. Moral: If something seems too good to be true, it isn't. Google "Lottery scams."

## **ALL THE RESOURCES YOU NEED. ALL IN ONE PLACE.**

Even though you may take every possible precaution, identity theft can still happen to you. Consider these suggestions:

- Report the crime to the police immediately and get a copy of the police report.
- Keep a record of all conversations with authorities, lending and financial institutions, including names, dates, and time of day.
- Call your credit card issuers immediately, and follow up with a letter and the police report.
- Notify your bank immediately.
- Call the fraud units of credit reporting agencies to place a fraud alert on your name and SSN.

## **RESOURCES**

- Equifax:  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)
- Experian:  
1-888-397-3742  
[www.experian.com](http://www.experian.com)
- TransUnion:  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)
- Federal Trade Commission:  
1-877-IDTHEFT (877-438-4338)  
[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)
- Privacy Guard:  
1-866-482-7363  
[www.privacyguard.com/frank](http://www.privacyguard.com/frank)
- Privacy Rights Clearinghouse:  
1-619-298-3396  
[www.privacyrights.org](http://www.privacyrights.org)
- Fight Identity Theft:  
[info@fightidentitytheft.com](mailto:info@fightidentitytheft.com)  
[www.fightidentitytheft.com](http://www.fightidentitytheft.com)
- Identity Theft Resource Center:  
1-858-693-7935  
[www.idtheftcenter.org](http://www.idtheftcenter.org)
- National White Collar Crime Center:  
1-800-221-4424  
[www.nw3c.org](http://www.nw3c.org)
- Social Security Administration  
1-800-269-0271  
[www.socialsecurity.gov](http://www.socialsecurity.gov)
- U.S. Postal Service:  
1-800-275-8777  
[www.usps.com/postalinspectors](http://www.usps.com/postalinspectors)

