

IDENTITY THEFT: DON'T BE A VICTIM!

**Edward J. McMillan, CPA
Post Office Box 771
Forest Hill, MD 21050
Telephone & FAX: 410/893-2308
Email: emcmillan@sprintmail.com
Website: www.nonprofitguru.com**

IDENTITY THEFT

What can an Identity Thief do with your personal information?

- Go on spending sprees using your credit and debit card account numbers to buy “big-ticket” items that can easily be re-sold.
- Open new credit card accounts, using your name and so forth. When they don’t pay the bills, the delinquent accounts will affect your credit.
- Change the mailing address on your credit card account and run up that account because the bills are being sent elsewhere.
- Purchase cars in your name.
- Establish telephone service in your name.
- Drain your bank account by printing counterfeit checks.
- Open up checking accounts in your name and pass bad checks.
- File for bankruptcy in your name to avoid paying debts they have incurred or to avoid eviction.
- Give your name to the police during an arrest. When they don’t show up for a court date, an arrest warrant may be issued in your name.

What steps should I take to prepare myself in advance in the event my identity has been stolen?

Take a few minutes to capture important information and keep it in a safe place and immediately available:

1. Go to a copying machine and make a *copy* of all the important information in your purse or wallet, including:
 - All of your credit cards.
 - Your ATM Cards.
 - Your Debit Cards.Next to this information, jot down the telephone numbers noted on the back of the cards to call to report lost or stolen cards.
 - Your Driver’s License.
 - Important insurance information.
2. Write down all of your bank account numbers, including checking accounts, savings accounts, certificates of deposit, lines of credit and so forth. Next, visit your bank and write down your branch telephone number, local contact name and national telephone number to call to report fraud.
3. Visit your local Police Department and write down their telephone number to report fraud.
4. Write down the address and telephone number of your attorney.

5. Write down names, account numbers, contact names and telephone numbers for your retirement trustee, investment agents, etc.
6. Write down the names, policy numbers, agent's names and telephone numbers for your insurance policies.
7. Write down the names, addresses and telephone numbers of the three major credit bureaus to place a fraud alert:

Equifax 1-800-525-6285
PO Box 740241
Atlanta, GA 30374-0241

Experian 1-888-397-3742
PO Box 9532
Allen, TX 75013

TransUnion 1-800-680-7289
Fraud Victim Assistance Division
PO Box 6790
Fullerton, CA 92834-6790

8. Write down the telephone number of your state Motor Vehicles Administration to report your card has been stolen.
9. Call the Social Security Administration Fraud Hot Line: **800-269-0271**
10. Contact the major check verification companies and ask that retailers not accept your checks:

TeleCheck 1-800-710-9898

Certegy 1-800-437-5120

International Check Services 1-800-631-9656

11. Call SCAN to see if anyone has been passing bad checks in your name:

1-800-262-7771

12. File a complaint with the Federal Trade Commission (FTC), by calling:

FTC Identity Theft Hotline 1-877-438-4338

13. Get a second photo ID, such as a duplicate Driver's Licenses or Passport. This is particularly important when traveling out of town, as a photo ID is required to board airplanes, enter buildings, etc.

****/Okay, you're prepared now and if you should unfortunately find yourself the victim of Identity Theft, this is the course of action you should be prepared to take immediately:***

1. File a police report in the jurisdiction where it was stolen and make sure to get a copy of the report.
2. Contact the three major credit bureaus.
3. Contact your credit card companies.
4. Call your bank and have it freeze all of your accounts.
5. Call the Department of Motor Vehicles.
6. Contact the major check verification companies.
7. If necessary, change the locks on your house and car.
8. Complete an **ID THEFT AFFADAVIT**. Follow up on items 2 through 6 and see if it is necessary to file it with these organizations.
9. File a complaint with the FTC.

How is someone's identity typically stolen?

- They get information from employers and business institutions by stealing records, bribing employees, hacking computers, etc.
- They rummage through your trash.
- They obtain credit reports.
- They steal wallets and purses.
- They steal mail.
- They complete "change of address forms" and divert mail.

- They break into your home.
- They scam information by posing as government officials, pollsters, etc.

What are the best ways to *protect yourself* from Identify Theft?

Several and they are *all* very important:

1. Never use the mailbox outside your home to mail bills unless it is secured.
2. Consider getting a Post Office Box and have important information such as bank statements, credit card bills, retirement statements and the like mailed there instead of your home.
3. Shred or rip up unsolicited pre-approved credit cards, loans, etc.
4. For personal checks, use your initials and last name and your Post Office Box address:

**E. J. Prosperous
Post Office Box 701
Baltimore, MD 21201**

Note: After having checks preprinted similar to the above, go to your bank and sign your *signature cards* using your full name. This way, if someone should come into contact with your checks, they would not know your first and middle names or how you sign your checks. This is of particular importance to women, as checks would not note your home address.

5. Never print your Social Security Number, Driver's License Number, home telephone number, etc. on your checks.
6. Get the type of check stock that can't be scanned.
7. If you write a lot of checks, consider the bank's Positive Pay service.
8. When you pay credit card bills, don't write your full account number on the check; only note the last four digits.
9. Consider paying your credit card bills, mortgage payment, etc. by Cashier's Checks or Money Orders instead of personal checks.
10. Try to use On-Line Banking, Debit Cards, and Credit Cards as often as possible – they are actually much safer than checks.

11. When dealing with merchants that use Electronic Check Conversion, be sure to get your original check back.
12. If your employer offers Direct Deposit for payroll, take advantage of it.
13. Use Debit Memorandums to pay certain expenses such as insurance premiums, car payments and so forth.
14. Open your bank statements and credit card bills *immediately*. Remember, if your account has been compromised, you have an obligation to advise the institutions or you may end up absorbing some or all of the loss.
15. Be creative when deciding on a PIN, and avoid the following:
 - Your initials.
 - Your birthday.
 - Your home address.
 - Your home telephone number.
 - Your Social Security number.
 - Your mother's maiden name.
 - Consecutive numbers such as 1-2-3-4, 3-3-3-3 etc.
16. Get a copy of your Credit Report.
17. Certain hotels capture personal information such as your name and credit card number on the hotel room key. Take the key with you and destroy it.

Computer Issues:

1. Update your virus protection regularly.
2. Don't download files from strangers.
3. Use a firewall.
4. Use a secure browser.
5. Don't respond to unsolicited emails.
6. Be careful when clicking on links from unsolicited emails.
7. Don't share your password.
8. Be careful to remove personal information when selling, trading-in, trashing your computer.

What can someone do with my Social Security number?

1. Get a Driver's License in your name.
2. Take out loans in your name.
3. Get credit cards in your name.
4. Finance a car in your name.