PROTECTING YOURSELF FROM IDENTITY THEFT

The Office of the Attorney General of Maryland
Identity Theft Unit
1) What is Identity Theft?

2) How to Protect Yourself From ID Theft.

3) How to Tell If You Are a Victim.

4) How to Recover From ID Theft.

5) Additional Resources.
When someone uses your personal information to obtain goods or services without your permission

Identity theft is one of the fastest growing crimes in the country, affecting nearly ten million Americans a year, and Marylanders are not immune.

Victims often spend hundreds of hours and thousands of dollars to fix the damage caused by ID Thieves.
WHAT IS Identity Theft?

- Financial Identity Theft
  - Existing account fraud
    - Bank accounts
    - Credit Fraud
  - New account fraud
    - Credit cards, loans, bank accounts
    - Utility/cell-phone accounts
WHAT IS IDENTITY THEFT?

- Financial Identity Theft
  - Government document fraud
    - Driver’s license
    - Social security
  - Other Fraud
    - Jobs
    - Apartment Rentals
Medical Identity Theft:

- An unauthorized person uses your personal information to receive medical care.
- An unauthorized person uses your insurance information or Medicare/Medicaid information to pay for medical care.
What Is Identity Theft?

Medical Identity Theft:

- Why is this dangerous?
  - Negatively affect your insurance rates, etc.
  - Could lead to an inaccurate diagnosis or dangerous drug interaction.
“Criminal” Identity Theft:

- A person uses your personal information in the commission of a crime.
  - As an alias.
  - During a traffic stop.
Identity thieves obtain personal information by:

- Stealing wallets and purses,
- Stealing mail,
- Completing a “change of address” form to divert your mail to another location,
- “Dumpster Diving” for documents with personal information,
- Stealing files from businesses where they work or by hacking into electronic files.
What Is Identity Theft?

Identity thieves obtain personal information by:

- “Phishing” or sending emails that appear to be from legitimate businesses asking for a consumer’s personal information,
- “Skimming” or using special storage devices to steal your credit or debit card number when they process your card,
- “Pretexting” or using false pretenses to obtain your private information from your bank, phone company, or even you.
1) Protect Your Personal Information
   1) At Home
   2) On The Go
   3) Online

2) Monitor Your Accounts to Look For Signs of Fraud
PROTECT YOUR PERSONAL INFORMATION AT HOME

Opt-out

- Pre-screened credit card offers,
  - Call 1-888-5-opt-out (567-8688),
  - Or go online: www.optoutprescreen.com

- Junk mail,
  - Write to: Mail Preference Service
    Direct Marketing Association
    P.O. Box 643
    Carmel, NY 10512
  - Or go online: www.DMAChoice.org
PROTECT YOUR PERSONAL INFORMATION AT HOME

Don’t give out your personal information

- Over the phone,
- Through the mail,
- Over the Internet,
- Unless you initiated the contact and know you can trust the person on the other side.
Protect Your Personal Information At Home

Buy a shredder

- destroy any documents that contain personal information instead of throwing them away.
  - Credit card offers you receive in the mail,
  - Bank and credit card statement statements,
  - Phone and utility bills,
  - Medical documents
  - Any documents that contain your sensitive personal information.
Use a locking mailbox to prevent mail theft.

Use passwords and PIN numbers for your credit card, bank, and phone accounts.

Use a safe to secure personal information in your home.
Don’t carry sensitive information in your purse or wallet

- Social Security Card,
- Bank account PIN,
- Insurance cards,*
- leave them at home in a secure place.
Make copies of important documents.

- Photocopy your credit cards front and back as well as your Social Security card and insurance cards.
- If your wallet is stolen, you will have all the information at home if you need to close those accounts.
Don’t give out your Social Security Number

- Unless it is absolutely necessary,
- Sometimes you will be required to use your SSN, for tax purposes, Medicare, or to request a credit report from the credit bureaus,
- If you have a membership card that uses your SSN, ask for a randomly generated ID number instead.
Be wary of e-mail scams.

- Financial institutions never ask for personal info by e-mail.
- Scam artists will use many tactics to trick you into sending them your personal information, or clicking on a link that contains a virus.
- Delete any suspicious messages immediately.
- Or forward them to spam@uce.gov
Don’t access sensitive information on the Web

- Unless you know the connection is secure.
  - Security enabled wireless networks
  - Hard wired connections
- Public Wi-Fi networks can be hacked.
Credit Cards v. Debit Cards

- Federal laws protect you from fraudulent charges on your credit cards.
  - $50 if you report within 60 days.

- Debit cards are NOT credit cards*

- Federal law protects you from fraudulent bank withdrawals.
  - $50 if you report within 2 days
  - $500 within 60 days
  - All of it after 60 days
Monitor Your Accounts To Look For Signs of Fraud

- **Review your credit report:** Under Maryland and federal law, you are entitled to two FREE credit reports from each of the Credit Bureaus per year.

- **Look for:**
  - New accounts that you didn’t open,
  - Accounts in bad standing,
  - Excessive credit inquiries.
Call 1-877-322-8228 or go to www.annualcreditreport.com to access your report through the Federal law.

Contact each of the Credit Bureaus to access your report through MD state law:

- Equifax: 1-800-685-1111,
- Experian: 1-888-397-3742,
- Trans Union: 1-800-680-7289.
Contact each of the Credit Bureaus to access your report through MD state law:

Monitor your bank, credit and utility accounts.

- Keep an eye out for fraudulent charges or withdrawals.
- Time limits
Common signs of Identity Theft include:

- Your bank or credit card statements never arrive in the mail,
- You receive acknowledgments of new accounts opened that you do not recognize,
- You receive calls from collection agencies demanding payment for accounts you never opened or purchases you never made.
Common signs of Identity Theft include:

- Mysterious charges on your credit card bill,
- Accounts appear on your credit report that you did not open,
- You are denied credit or offered less favorable credit terms, such as high interest rates.
- There are warrants out for a crime committed in your name.
HOW TO RECOVER FROM ID THEFT

1) Steps To Take To Recover

2) Tips For The Recovery Process

3) Credit Monitoring and ID Theft Protection Services
Place a fraud alert on your credit report

- Call one of the three Credit Bureaus, Federal law requires them to tell the other two that you have placed the fraud alert:
  - Equifax: 1-888-766-0008
  - Experian: 1-888-397-3742
  - Trans Union: 1-800-680-7289

- You will be sent a free credit report, review it for fraudulent activity.

- A fraud alert warns creditors that you maybe a victim of fraud and to confirm your identity when issuing credit in your name.*
File a police report.

- Maryland law requires your local law enforcement agency take a police report for identity theft and give you a copy.
- You will need a police report for several of the following steps.
- Use the FTC's general complaint form and make sure all the relevant info is included.
How To Recover From ID Theft

File a complaint with the Federal Trade Commission

- www.ftc.gov/idtheft, 1-877-382-4357
- Fill out an ID Theft Affidavit.

Call the ID Theft Unit

- We provide:
  - Materials,
  - Advice,
  - Contact info for other organizations with resources for ID theft victims.
Dispute Fraudulent Accounts

- Close any accounts opened fraudulently.
- Send a request in writing for all account records to be sent to you. Federal law requires a business to provide you with all account information if you have a police report.
How To Recover From ID Theft

- Dispute Fraudulent Charges In Writing
  - Existing bank, credit, utility accounts
    - Change your account numbers and order new credit cards and checks,
  - Any information relating to fraud that appears on your credit report,
  - Contact the ID Theft Unit for sample dispute letters and instructions.
Apply for an Identity Theft Passport. The passport can be used to help prove to creditors that you do not owe money on fraudulent accounts, and help prevent an accidental arrest if an ID thief used you as an alias.

- Go to www.oag.state.md.us/id_theft for an application.
“Freeze” your credit report:

- The “freeze” completely blocks the information on your credit report from new creditors. Most businesses won’t open credit accounts without first checking your credit history.

- Contact each of the three credit bureaus to place the freeze.

- A credit freeze is free to ID theft victims with a police report, and MD law prohibits the credit bureaus from charging more than $5.
Medical ID Theft:

- Follow the same steps as for financial ID theft;
  - File a police report,
  - Dispute fraudulent charges,
    - You will have to prove that it was not you who was provided the medical care,
    - Get a letter of clearance once you have fixed the problem.
Medical ID Theft:

- Correcting misinformation on your medical record;
  - Ask to see a copy of your medical record under HIPAA,
  - Place a red flag on your medical file through your regular doctor,
  - Request amendments to your file to remove the fraudulent information.*
“Criminal” ID Theft:

- Contact the State’s Attorney’s office in the jurisdiction where the crime was committed,
- Explain that you are a victim of identity theft, and ask them what steps you need to take to clear your name,
- Find your county’s State’s Attorney at this website: www.mdsaa.org.
Remember these tips when fixing damage caused by ID thieves:

- Write down the name of anyone you talk to, what s/he told you and the date of the conversation,
- Follow-up in writing. Use certified mail, return receipt requested,
- Keep copies of all correspondence or forms relating to the ID theft,
- Keep the originals of supporting documentation, like police reports and letters to and from creditors; send copies only,
- Keep old files even if the problem is resolved. If it happens again, you'll be glad you did.
Recent headlines about security breaches and loss of personal info have encouraged many businesses to offer ID theft protection programs.

These usually contain:

- Credit monitoring services that alert you to any activity on your credit report,
- Recovery services or ID theft insurance to help should you become a victim
Credit Monitoring and ID Theft Protection Services

- Be sure to read any service contract thoroughly before signing up.
  - Many of the services provided by these companies can be performed by you for free,
  - they can be useful if you do not have time to perform these tasks yourself.
The Office of the Attorney General does not endorse any specific identity theft protection company.
In January 2008, the Maryland Personal Information Protection Act (PIPA) went into effect.

- Requires businesses now notify MD residents if their personal info is compromised.
- Requires the businesses to notify the OAG
- Visit www.oag.state.md.us/idtheft to see all security breaches received by the OAG
Place a fraud alert,

Monitor your credit report,

Close any affected accounts;
  - Ask for new cards with new numbers,
  - Place red flags on your bank accounts,

“Freeze” your credit reports,

Call the OAG ID Theft unit.
The Attorney General’s Identity Theft Unit can help victims of ID theft address their problems and help all consumers to protect themselves against ID theft.

You can contact the Identity Theft Unit by:

- (410) 576-6491 or 1-888-743-0023
- idtheft@oag.state.md.us
- www.oag.state.md.us/idtheft
The FTC:
- 1-877-382-4357, www.ftc.gov/idtheft

The Identity Theft Resource Center is a non-profit organization that helps victims recover:
- (858) 693-7935, www.idtheftcenter.org

The Privacy Rights Clearinghouse offers information on ID theft and privacy issues:
- (619) 298-3396, www.privacyrights.org

The Md. Crime Victim’s Resource Center
- 1-877-842-8461, www.mdcrimevictims.org