Office of
CONSUMER AFFAIRS
Howard County Department of Citizen Services

MINIMIZE YOUR RISK FOR IDENTITY THEFT

Con artists want your identity to: steal money, access credit or health care, get a tax refund, or even commit crimes.

Look out for the warning signs of identity theft

- Bank account withdraws that you didn't make;
- Letters or debt collector calls for bills you don't owe;
- Health insurance claims for treatments you didn't receive;
- Accounts listed on your credit report that you didn't open
- A notice from the IRS that a return was filed in your name.

While there is no way to guarantee you won't be the victim of ID Theft, there are steps you can take to reduce your risk.

Personal Safety

- Never provide personal information unless you know who you are dealing with and how it will be used.
- Do not carry credit cards, social security card, passport, and other forms of personal identification that you don't regularly use.
- Take your receipts from all bank machines, gas pumps, and retail stores.

Mail Safety

- Review your bills for any charges you did not authorize and health insurance statements for claims that don't match the treatments you received;
- Pay attention to credit billing cycles. If bills don't arrive on time, contact your creditor. A missing bill could mean that a thief has hijacked your account and changed the billing address.
- Shred all mail and documents you don't need that contain personal information such as: pre-approved credit applications, credit card receipts, bills and medical statements.
- Do not send checks from your home mailbox. Promptly remove mail from your mailbox after it is delivered. For even greater protection, use a locking mailbox, or a PO Box for mail delivery.

Internet Safety

- Password-protect your credit and other financial accounts and chose passwords and security questions that only you will know.
- Only make purchases from secure websites. Look at the website's URL to see if it begins with "https" (the s stands for secure).
- Install virus protection and security software from a reputable company. Update that software regularly, using only the directions given by the company when you purchased the software.

- Beware of e-mail or pop-up messages that instruct you to click on a hyperlink or download software to verify your account information. Banks and other creditors don't make such requests. If you want to be sure, call the creditor using contact information on your bills.

Social Media Safety

- Read privacy and security policies closely to know what information the site sells or gives to others. Use the highest level privacy setting available on the site.
- Provide the least amount of information necessary to register for the site, and never include personal information (e.g. address or birth date) in your screen name or in posts.
- Be cautious about accepting invitations to connect from unfamiliar contacts, and verify the messages you receive. Scammers have been known to pose as friends or relatives.

Monitor Your Credit Report Regularly

- Request your credit report from all three of the major reporting agencies annually. Review them all at the same time or look at one every four months at www.annualcreditreport.com.
- Look for accounts you didn't open and activity on accounts you've closed. Review personal information (such as your current address) to make sure it's correct.
- Consider requesting a security freeze. Creditors will not approve credit applications without first reviewing that applicant's credit report. A security freeze keeps others from seeing the report. You must contact each reporting agency (Equifax, Experian, Transunion) to place a freeze on the reports they generate.

Pay Attention to Reports of a Data Breach

- Unfortunately, the personal information kept on file by companies or government agencies for legitimate purposes may be exposed by accident or stolen by hackers. If you receive a notice of a data breach, read the information carefully to minimize your risk
- In response to the data breach, you may be offered an ID theft protection service at no charge for some period of time. The service can help you monitor your accounts and alert you to new accounts opened in your name. When the free period of service ends, don't automatically agree to continue the service for a fee. You may, instead wish to monitor your accounts yourself for free.

If you believe you the victim of Identity Theft

- Contact the companies where you know fraud occurred
- File a police report
- Place a fraud alert on your credit reports. This lets creditors know to be suspicious of new applications. The alert stays on your report for 90 days, but you can have the alert extended for up to 7 years if you have a police report of the theft.
- Consider placing a security freeze on your reports.
- Report the identity theft to the Federal Trade Commission (FTC) and follow the suggestions given at the FTC's website: www.identitytheft.gov.
- Contact the Office of Consumer Affairs for more information or assistance.

To obtain this factsheet in an alternative format, please contact the Office of Consumer Affairs at 410-313-6420(voice/relay) or email us at consumer@howardcountymd.gov.