IDENTITY THEFT

AWARENESS, PREVENTION & RECOVERY

IDENTITY THEFT/FRAUD: Identity Theft/fraud involves acquiring key pieces of someone's identifying information such as; name, address, date of birth, social security number and mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous types of fraud which include but are not limited to; taking over the victim's financial accounts, opening new bank accounts, purchasing automobiles, obtaining mortgages, applying for loans, credit cards, and social security benefits, obtaining fraudulent driver's licenses, getting arrested and creating an erroneous criminal record, renting apartments and establishing services with utility and phone companies.

The Federal Trade Commission (FTC) recently released a report indicating Identity Theft has increased in Maryland by 188% since the beginning of 2020. That is a staggering statistic. It is important to safeguard your personal identifying information and never share passwords.

IF YOU'VE BEEN A VICTIM OF IDENTITY THEFT,
IMMEDIATELY TAKE THE FOLLOWING STEPS:

- File a police report in the jurisdiction where you live or where the crime occurred
- Contact all of your creditors and banks, and alert them of the fraud
- Place a fraud alert with all 3 major credit bureaus
- Obtain a free copy of your credit report
- File a complaint with the Federal Trade Commission (FTC)

BENEATH THE STATISTICS

In May 2002 a New Jersey woman received a notice from a North Carolina police department. The notice stated her husband had just committed a traffic violation in North Carolina. The problem… The woman's husband died 8 months earlier in the World Trade Center on September 11, 2001. Renewing hope that her husband was alive, this woman contacted the police department that issued the notice, only to discover that a thief had stolen her husband's identity. (Robin Gaby Fisher, "Identity Theft robs name of 9/11 victim," – Star-Ledger, September 22, 2002)

Derek, a Caucasian male mail carrier in Maryland attempted to purchase a vehicle. He was informed that he could not obtain financing due to the fact that he already owned a 2000 Mercedes. The Investigation revealed that an unknown (African American) male had acquired his social security number and provided the car dealership with a fraudulent DC driver's license. (Case files of the ID Theft Unit)

Serena, a woman from Anne Arundel County, Maryland and her husband applied for a new home loan. The loan was denied due to thousands of dollars in unpaid medical and cable service bills. The investigation revealed that an ex-friend had received medical attention at a local hospital and also obtained Comcast Cable services under her name. In both cases, her social security number was used. (Case files of the ID Theft Unit)

A female from Baltimore City had filed an application for Public Housing assistance. Her application was denied due to several charges appearing on a criminal record check, which was completed by a name query only. The investigation revealed that someone else had been arrested and used her name. Upon obtaining a copy of the arrest photograph and fingerprint information, it was clear that this was not the same person that had applied for assistance. The woman was given a letter of explanation from the State's Attorney's Office and her application was then approved.

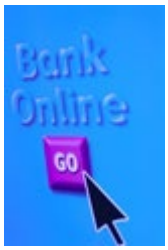
Travon, a college graduate in Baltimore County was arrested on a bench warrant for not appearing in court regarding serious traffic charges that were actually issued to Earl, the father of his sister's child. Earl had used Travon's name on 22 separate occasions relating to traffic violations in Baltimore City and County. Travon missed countless days from school and after graduation, his job, due to appearing in court for all of the erroneous traffic violations. Earl was prosecuted and found guilty on several occasions. He also spent time in jail. After being released, he used Travon's name yet again. On April 26 2006, Earl was sentenced to 5 years in jail.

"PHISHING"

PHISHING (fish' ing) The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The web site, however, is bogus and set up only to steal the user's information. For example, 2003 saw the proliferation of a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the provided link and updated the credit card information that the genuine eBay already had. Because it is relatively simple to make a web site look like a legitimate organization's site by mimicking the HTML code the scam counted on people being tricked into thinking they were actually being contacted by eBay and were subsequently going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with eBay legitimately.

UNI-BALL PENS

Many Uni-ball pens, including the Uni-ball Signo 207 gel pen, the Jetsream, Jetstream RT and Vision Elite roller ball pens, use specifically formulated inks that contain tiny color pigments. This exclusive "Super Ink" helps prevent document and check fraud by absorbing into the paper fibers. When an individual tries to wash or lift the inked information written on the document, the ink remains "trapped" within the fibers of the paper, thereby deterring the efforts of identity thieves.



FISHING FOR "PHISHERS" (ONLINE BANKING)

"Phishing" e-mails are being sent from a site designed to look like your bank site. In some cases you don't even have an account with the bank that is sending you the e-mail. The e-mail advises that the company is updating their files and requests that you log on. After doing so, it asks for your account name, account number, PIN and sometimes a social security number. The e-mail request may be similar to the following:

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity." **or** ***"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."***

Never e-mail personal or financial information. E-mail is not a secure method of transmitting personal information. **Banks do not use this practice for updating information.**

Forward spam that is phishing for information to spam@uce.gov and forward a copy to the company, bank or organization that has been impersonated in the phishing e-mail. Most organizations also have information on their websites about where to report problems.

If you believe you've been scammed, file your complaint at **ftc.gov**, and then visit the Federal Trade Commission's Identity Theft website at www.consumer.gov/idtheft Victims of phishing can become victims of identity theft. The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and helps consumers spot, stop and avoid them. To **file a complaint** or to get other free information on consumer issues, log onto www.ftc.gov or call toll-free at 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters on-line, telemarketing, identity theft, and other fraud-related complaints into **Consumer Sentinel,** a secure, online database available to criminal law enforcement agencies in the U.S. and abroad. For further information, visit www.consumer.gov/sentinel

THE CREDIT CARD SWITCH

One of the more recent scams reported is the **credit card switch.** When your credit card is returned, the fraudster will give you back someone else's and keep yours. Check to make sure your own card has been returned. In most instances you do not notice the card has been switched until days or weeks later. In conjunction with a credit card sale, never put your address, telephone number or driver's license number on the receipt. Do not leave your signed credit card receipt on the table or counter at a restaurant. It may contain your entire account number and someone can easily obtain your information.

SKIMMING

"Skimming" Identity thieves purchase a portable card reader and place it directly next to the cash register where they are working. The **"phony"** card reader is then connected to a laptop computer, which is usually placed under the counter. When your card is swiped, your name, account number and expiration date appears on the screen. The card is then swiped a second time through the **"genuine"** register card reader. You may notice that after the clerk swipes the card the first time through the **"phony"** card reader, they will wipe the magnetic strip to pretend that it is smudged and unreadable. They will then swipe it through the **"genuine"** card reader the second time. **If this happens to you, insist on speaking with the Manager.**

Another type of skimming occurs when you are in an environment (i.e. restaurant) where your credit card is taken out of your sight. A portable skimmer is hidden in the wait staff's pocket. Your card is skimmed and the information is sent to an IPOD (about the size of a deck of playing cards), which stores your information and now the identity thief has it.

A former scam in Baltimore City involved alleged representatives from a cigarette company handing out free packs of cigarettes at nightclubs. In order to receive them the person had to provide a driver's license to verify their age. The problem…..the representatives were then scanning the driver's license and storing the information in an IPOD.

"TRAPPING" YOUR ATM CARD AND "SHOULDER SURFING"

Be careful at ATM's. Identity thieves can sabotage the machine by placing a sticky substance inside to trap your card. The thief will then **"shoulder surf"** by using binoculars or a zoom lens on a video camera to obtain your PIN. Once you are unable to retrieve your card and have left the area, the identity thief removes it with a hook tool. They now have your ATM card and PIN. The identity thief can wipe out your account before you have an opportunity to report it.

Your ATM card is stuck in the machine. You have tried everything. A stranger suddenly appears pretending to be helpful. They indicate that this also happened to them. They'll tell you that they entered their PIN number and either pressed the "*ente*r" or "*cancel"* key and the card suddenly came out. They encourage you to do the same, several times if necessary. They have watched you enter your PIN and once you have left the area, they retrieve the card and wipe out your account.

The **"shoulder surf"** scam can also happen if you are at a public phone and are entering your credit card number on the keypad. As you enter your card and PIN the identity thief may be recording your actions on a video camera with a zoom lens. After they have your information, they can order items using your credit card and PIN.

BEWARE OF CELL PHONE CAMERAS

Cell phone cameras are everywhere and they're taking pictures of your information!!!!!

Imagine walking along and someone approaches you with a wallet in their hand and asks if you've lost yours. You check and your wallet is missing. The wallet the scammer is holding turns out to be yours and amazingly, your driver's license, credit cards and even the cash is all still there. What you don't know is that you were pick-pocketed and the fraudster took a picture of the contents with their cell phone camera. Now they have all of your personal identifying information to use as they please.

MAIL THEFT

Do not place outgoing mail in your home mailbox, especially checks. A "**raised pick-up flag"** is like a **"steal me"** sign to an identity thief. Always deposit mail in the blue U.S. Postal mailboxes or take it to the Post Office. Mail theft is common and it is easy to change the recipient on a check with an acid wash. Your incoming and outgoing mail may contain a lot of personal information (i.e. name, date of birth, credit and bank account numbers, etc.) For incoming mail, try to get a locked mailbox or use a Post Office box if possible.

If you have moved, immediately provide a new address to friends, relatives and businesses. Don't rely on mail forwarding, which may put your mail at greater risk of theft. Also, refrain from putting account numbers on the outside of the envelope. It is a federal offense to tamper with the U. S. mail. If you suspect your mail has been tampered with, contact the U.S. Postal Inspection Services on the web at www.usps.gov/postalinspectors or by phone at 410 715-7700.

Pay attention to billing cycles and inquire about credit bills that do not arrive on time. They may have been misdirected by identity thieves. It is easy for the thief to change your mailing address over the phone or online.

When you order a new credit card or your previous one has expired, watch the calendar to ensure you receive it at the proper time. If you do not receive it within that time frame, contact the credit card grantor immediately and ascertain if the card was sent, and to what address. Find out if a change of address was filed.

The Jury Duty Scam

You receive a phone call indicating you have missed jury duty. The caller indicates this is a serious offense and you must provide your name, date of birth, address and **social security number** in order for them to research your records to resolve the matter **Don't release your information. It's a SCAM!!!**

DUMPSTER DIVING

A Social Security number is like having the "keys to the kingdom."

Identity thieves regularly peruse personal and corporate trash and recycling bins for anything with your name, DOB, address, social security number, driver's license number, etc. on it. Do not discard or recycle anything containing your personal identifying information. Ask financial institutions, doctor's offices, hospitals, car dealerships and other types of businesses what they do with your private information. Tell them why they need to protect your information while it is being stored in their facility and shred it after they no longer need it. A financial institution (i.e. when applying for a loan, opening a bank account, applying for a mortgage) and your employer must have your social security number. Other types of companies do not need it to identify you. If a business asks for your social security number, inquire why they need it and how it will be used. Request that an alternate number be used. If a governmental agency requests your social security number, there must be a privacy notice accompanying the request.

Many insurance carriers use your social security number as a policy number. In an effort to address the issue of identity theft, Blue Cross & Blue Shield and other insurance carriers have now issued a different identifying number. If you have an insurance carrier that still uses your social security number, ask if your number can be changed.

SHRED, SHRED, SHRED

Shred, shred, shred all of your important papers, especially pre-approved credit card applications/offers/cards, medical paperwork and other documents containing your identifying information. If you don't have access to a shredder, tear or cut up your documents into small pieces and throw them in separate trashcans.

If your social security number is fraudulently being used, contact the Social Security Administration's Office of the Inspector General - fraud hotline at 1-800-269-0271.

OPT OUT PRESCREENED OFFERS

If you decide that you don't want to receive prescreened offers of credit and insurance, you have two choices: You can opt out of receiving them for five years or opt out of receiving them permanently. Call toll-free 1-888-5-OPTOUT (1-888-567-8688) or visit www.optoutprescreen.com for details. The telephone number and website are operated by the major consumer reporting companies. When you call or visit the website, you'll be asked to provide certain personal information, including your home telephone number, name, Social Security number, and date of birth. The information you provide is confidential and will be used only to process your request to opt out. (source – ftc.gov)

TELEMARKETING

To remove your home and cell phone number from the telemarketing phone lists, write to the following address or simply log onto the website as follows:

Direct Marketing Association
Telephone Preference Service
P.O. Box 9014
Farmingdale, NY 11735
www.donotcall.gov

Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, etc., unless you initiated the phone call.

EMPTY YOUR WALLET AND COPY, COPY, COPY

Empty your wallet of all extra credit cards, etc. that you do not need. Do not carry your birth certificate, social security card or passport, unless absolutely necessary.

Photocopy the **front** and **back** of all necessary cards/identification carried in your wallet (credit cards, driver's license, medical cards, bankcards, etc.) and put the copy in a safe place. If your wallet is lost or stolen, you will have direct access to all account numbers and customer service phone numbers. Notify everyone immediately and place a ****fraud alert*** (explained on the next page) with all 3 Nationwide Credit Reporting Agencies. You may also want to cancel the compromised accounts and open new ones. If your wallet is lost or stolen, file a police report right away.

If you have credit accounts that are not being used, close them. Contact the credit company and be sure to get a confirmation that the account has been closed. Cut up or shred unused credit cards. Unused credit is a prime target for identity thieves. (Closing an account may adversely affect your credit score)

The next time you order checks, do not put your full name on them. Use your first initial and last name. If your checks are lost or stolen and someone tries to use them, they will not know the correct full name to sign. You may choose to not sign the back of your credit cards. Instead write, **"See ID"** or **"Photo ID Required"** in permanent marker.

Try to get credit cards with your picture on them. FYI-some establishments, including the U.S. Post Office, will not accept an unsigned credit card.

PLACING A * *FRAUD ALERT* *
ON YOUR CREDIT REPORT

To place a ***Fraud Alert*** …….. Contact **Equifax**. Per the recorded message, once the fraud alert has been successfully placed with them, they will automatically contact **Experian** and **TransUnion** for you and the alert will also be recorded with their Agencies. Contact information as follows:

Equifax: **1-800-525-6285** www.equifax.com
P.O. Box 740241
Atlanta, Georgia 30374-0241

Experian: **1-888-397-3742** www.experian.com
P.O. Box 9532
Allen, Texas 75013

TransUnion: **1-800-680-7289** www.transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, California 92834-6790

There are 2 types of ***fraud alerts*…** an **initial**, and an **extended** alert.

- **An initial alert stays on for at least 90 days.** You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing "scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the 3 Nationwide Credit Reporting Agencies.

- **An extended alert stays on your credit report for 7 years.** You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the Credit Reporting Agency with a police report. When you place an extended alert on your credit report, you're entitled to 2 free credit reports within twelve months from each of the 3 Nationwide Credit Reporting Agencies. In addition, the Credit Reporting Agencies will remove your name from marketing lists for pre-screened credit offers for 5 years unless you ask them to put your name back on the list prior to the 5 year expiration.

When a business sees the alert on your credit report, they must verify your identity before issuing credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you're trying to obtain credit quickly. To compensate for possible delays, you may want to include a cell phone number in your alert where you can actually be easily reached. Remember to keep all contact information in your alert current.

Contact each individual creditor and ask to have passwords placed on your accounts. Do not use your mother's maiden name. Make up a fictitious word. Once you have placed an alert, you may be required to show a photo ID or other credentials when using a credit card to purchase items in person. When purchasing items via the telephone or online, you may be asked for a PIN. **Remember that this is for your protection.**

CREDIT REPORTS

A recent amendment to the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months. To order your free annual report from one or all of the national consumer reporting companies, visit www.annualcreditreport.com**, call toll-free 1-877-322-8228 or complete an Annual Credit Report Request Form (you can obtain a copy of the form at** www.ftc.gov/credit **and mail it to:**

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, Georgia 30348-5281

Once you have received the reports, review them carefully. If there are entries that appear to be fraudulent log onto the Federal Trade Commission's web site at www.consumer.gov/idtheft and follow the instructions. You may also call the FTC at 1-877-IDTHEFT. The web site contains an ID theft affidavit that is accepted by most companies. The web site also provides samples of letters to send to creditors, banks, etc. Always send letters via certified mail and keep a copy of all written correspondence, as well as, a log of the names and phone numbers of everyone you speak with. Per the FTC, once it has been determined that you are not the person that committed these fraudulent acts; the creditors are required to remove the entries from your credit report.

HOW CAN THE MARYLAND MVA HELP PREVENT IDENTITY THEFT?

APPLY FOR AN "R" DRIVER'S LICENSE RESTRICTION CODE

The Maryland Motor Vehicle Administration offers a voluntary program to assist victims of identity theft by placing an "R" driver's license restriction code that is displayed on the person's driver's license and driving record. If you have been the victim of an Identity Theft crime and would like to apply for the "R" restriction code, you must first file a report with the local law enforcement agency that has jurisdiction over:

1. any part of the county in which the person lives; or
2. any part of the county in which the crime occurred (MD Criminal Law 8-304) (copy of the law is on the next page)

The police report must indicate the type of incident/crime as Identity Theft/Identity Fraud. You will need to take a copy of the report to the MVA Headquarters located at 6601 Ritchie Highway, Glen Burnie, MD 21062, Investigative & Security Services Division – Room 53 and ask to speak with the Duty Chief Investigator. (Phone # 410-768-7541 or 410-768-7536) You must also take your current valid Maryland driver's license with you. After approval from a Chief Investigator, you will sign an authorization form (DL-204) granting MVA permission to place the "R" restriction code on your driver's license and driving record. After paying the applicable fee, you will then receive the driver's license displaying the "R" code.

HOW WILL THIS HELP ME?

If someone attempts to fraudulently use your name and identifying information during a traffic stop and does not physically have the driver's license displaying the "R" code, the law enforcement officer will be alerted that you have been a victim of Identity Theft. The officer should then attempt to further verify the identity of the individual.

POLICE REPORTS-IDENTITY FRAUD

Maryland Criminal Law – Code 8-304 (2005)

8-304 – Report

(a) Contact local law enforcement agency. A person who knows or reasonably suspects that the person is a victim of identity fraud, as prohibited under this subtitle, may contact a local law enforcement agency that has jurisdiction over:

(1) Any part of the county in which the person lives; or
(2) Any part of the county in which the crime occurred.

(b) Preparation of report. After being contacted by a person in accordance with subsection (a) of this section, a local law enforcement agency shall promptly:

(1) Prepare and file a report of the alleged identity fraud; and
(2) Provide a copy of the report to the victim.

(c) Referring matter to another law enforcement agency. The local law enforcement agency contacted by the victim may subsequently refer the matter to a law enforcement agency with proper jurisdiction.

(d) Not included as open case. A report filed under this section is not required to be counted as an open case for purposes including compiling open case statistics.

Cyber Security

- Use strong passwords such as a mixture of upper and lower case letters along with symbols and numbers in a random order. Don't use common words or names. A weak password can usually be decrypted within 15 minutes. If you have multiple passwords you may want to record them in a "password keeper" location on your phone or computer. Be sure the "password keeper" is also password protected.
- Never share passwords.
- Use a different password for each account. If you use the same one then the hacker has access to all of your accounts.
- If a website asks if you want to save the password, always click on "no".
- Regularly delete cookies/history in your web browser.
- Wi-fi on your personal computer should be password protected. Also, password protect your phone and computer.
- Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies.
- Always lock your computer when you are not at your desk.
- Never open an email from an unknown sender. If you are unsure, call the email sender to authenticate. (i.e. invitation to connect to LinkedIn, etc.) If the email contains an attachment, you may want to scan prior to opening.
- PDF files may contain viruses, or instructional code to upload a virus or key stroke logger to your computer.
- Don't click on a link contained in an email. Hover over the website address to ascertain if it is a legitimate site. Malicious websites sometimes use a variation in common spelling or a different domain.
- Never conduct banking or financial transactions or other transactions containing your personal information on a computer connected to public wi-fi (i.e. hotel, Starbucks, internet café, etc.)
- Websites requiring personal information such as banks, on-line shopping, etc. will begin with **https://**

- Thumb drives and digital photo frames may contain malware. Many times these thumb drives are given out for free at seminars and symposiums. There is a new scam involving cyber criminals loading thumb drives with malware and dropping them on the ground near business districts, shopping malls and other heavily travelled areas. When you plug it in to your computer, it becomes infected with the malware.
- **malwarebytes.org** provides information on free malware, virus, worms, trojans, spyware, etc. detection. There is also a paid version.
- Keep your laptop, thumb drive and cell phone secure at all times.
- Only download apps on your computer or phone from a reputable source. Advertisements offering free downloads usually contain malware and viruses.
- If a pop-up appears on the computer screen and asks you to click "yes", "no" or the "x" in the upper right-hand corner of the box, either enter "cntrl" "alt" "delete" and click on "end task" or click out of the browser entirely. Clicking on "yes", "no" or the "x" may upload malware, virus or key stroke logger to your computer.
- Turn your blue tooth off when not in use.
- When scanning documents from HP, Xerox, etc. to attach in an email, always send it to yourself first and then forward to the individual. Don't open an email sent directly from a scanner. Contact the sender first to ascertain if it is legitimate.
- Turn off the "geo-tagging" feature on your cell phone camera.
- Never carry your social security card with you.