

IDENTITY THEFT:

PROTECT YOURSELF, SECURE
YOUR FUTURE



CONSUMER PROTECTION DIVISION

MARYLAND OFFICE OF THE ATTORNEY GENERAL

IDENTITY THEFT: PROTECT YOURSELF, SECURE YOUR FUTURE

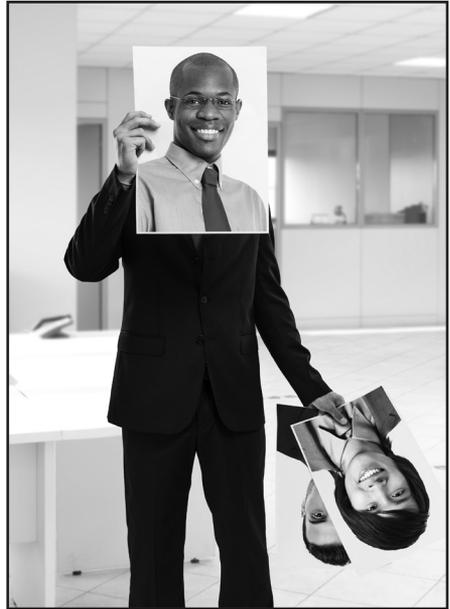
CONTENTS

The Basics.....	2
Be Proactive: How to Prevent Identity Theft.....	4
The Many Forms of Identity Theft.....	11
Take Action: What to Do if it Happens to You.....	16
Data Breaches: Reduce Your Risk.....	19
Additional Resources.....	21

THE BASICS

Identity theft is when someone uses your name or personal information to obtain goods or services without your permission. The most common forms of identity theft are financial account crimes, medical fraud, improper use of government benefits (including tax records) and impersonation of another individual.

It can happen when a criminal physically steals documents from your home, vehicle, mailbox, a purse or wallet, or wherever you keep important records. It can also happen when scammers intimidate or deceive consumers into revealing personal information, when cybercriminals hack into databases where sensitive data is collected and stored, or when consumers unknowingly share personal information through email and social media.



You can minimize the risk of becoming a victim by taking a few simple steps. Monitor your bills and statements, looking for unusual or unfamiliar activity, and be sure to check your credit report annually. You can further protect yourself through a fraud alert, credit freeze, enrolling in the Do-Not-Call registry, opting out of pre-screened credit card offers or other junk mail and simply shredding documents you no longer need. Additionally, don't give out any personal information unless you initiated the contact and only then to someone

you know and can trust. Be especially careful about supplying information over the phone or online.

Recognizing whether you're a victim can be easy when you take an active role in managing your finances and monitoring your consumer choices. Look for unusual activity or errors in your financial and health statements, credit reports and other records. Be wary of sudden changes in the amount of mail you receive, which could indicate stolen mail or unauthorized new accounts in your name. Another warning sign is if you receive less favorable interest rates than you anticipate or if you are inexplicably declined for a job or lease.

If you are an identity theft victim, there are ample resources to help you recover. At the state level, the Maryland Office of the Attorney General provides educational materials, sample letters, contact information, and help navigating the daunting road to restoring your identity. The Federal Trade Commission lets victims file a complaint that can be accessed by law enforcement agencies nationwide and it offers additional assistance for non-English speakers, as well as a wide variety of educational resources.



You may request a free copy of your credit report from each of the three nationwide credit reporting agencies – Equifax, Experian and TransUnion – once a year by going to <https://www.annualcreditreport.com>. This is one of the easiest and most effective ways to prevent identity theft. Maryland residents are entitled to an additional free credit report each year, which can be obtained by directly contacting any of the three credit reporting agencies

FREE CREDIT REPORT

Get your free credit report by going to
www.annualcreditreport.com, or by calling
1-877-322-8228.

AnnualCreditReport.com

The only source for your free credit reports. Authorized by Federal law.

EQUIFAX



Experian

TransUnion



BE PROACTIVE: HOW TO PREVENT IDENTITY THEFT

IDENTITY THEFT PREVENTION CHECKLIST

- Check your credit report annually
- Consider placing a credit freeze for yourself and family members
- Monitor financial statements and health records for suspicious activity
- Opt out of junk mail and pre-screened credit card offers
- Enroll in the Do Not Call Registry
- Shred unneeded documents containing personal information
- Prevent fraud by verifying the source of calls or emails before providing personal information
- Review your digital footprint by strengthening privacy settings and passwords, updating virus protection software and monitoring online purchases

FREE ANNUAL CREDIT REPORTS

A credit report includes some personal information as well as your financial history, such as whether you pay your bills on time and if you've filed for bankruptcy. Nationwide credit reporting agencies sell the information in your report to creditors, insurers, employers and other businesses that use it to evaluate your applications for credit, insurance, employment or renting a home.

CONSIDER A CREDIT FREEZE

A credit freeze or security freeze, which is different than a fraud alert, completely blocks the information on your credit report from would-be creditors or lenders.

Most businesses will not open credit accounts without first checking a consumer's credit history. Even someone who has your name and Social Security Number might not be able to get credit in your name if your credit files are frozen. Credit reporting agencies may not charge more than \$5 to freeze or unfreeze your credit report. Identity theft victims may freeze their credit reports at no cost.

While a credit freeze can protect against identity theft, it may not be for everyone. If you plan to open credit in the near future, or apply for an apartment or a job that will require your credit report to be checked, you will need to pay \$5 each time you want to lift the freeze – and \$5 to put it back in place.

OBTAIN A CREDIT FREEZE

Equifax

Phone: 888-298-0045

Online: http://www.equifax.com/help/credit-freeze/en_cp

Mail: Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348

Experian

Phone: 888-397-3742

Online: <https://www.experian.com/freeze/center.html>

Mail: Experian Security Freeze, P.O. Box 9554, Allen, TX 75013

TransUnion

Phone: 888-909-8872

Online: <http://www.transunion.com/securityfreeze>

Mail: TransUnion LLC, P.O. Box 2000, Chester, PA 19022

When sending by mail to any of the above, please include:

- Your full name, address, Social Security Number and date of birth; A copy of your police report if you are an identity theft victim eligible for a no-cost freeze; Prior addresses and proof of prior names if you have moved or had a name change in the past five years;
- Copy of a government-issued ID card; and
- Copy of a bank statement or utility bill containing your current address.

CHILD IDENTITY THEFT PROTECTION



In 2012, Maryland became the first state in the nation to give parents or guardians the ability to freeze a child's credit report so that the child is not victimized before he or she turns 18. When parents or guardians take advantage of this opportunity, they can ensure a child will begin his or her adult life with a clear credit history.

This law also applies to "protected consumers," which includes anyone under guardianship or conservatorship (e.g., someone with developmental disabilities or cognitive impairments). To find out who may be eligible for this protection, contact the Identity Theft Unit at 410-576-6491.

To place a credit freeze for your child, a parent or guardian must submit to the addresses listed below:

- The requestor's complete name, address, and any of the following: a copy of a Social Security card, an official copy of a birth certificate, a copy of a driver's license or any other government-issued identification, or a copy of a utility bill that shows the requestor's name and home address; and
- The child's complete name, address and any one of the forms of identification listed above.

Experian Security Freeze, P.O. Box 9554, Allen, TX 75013

Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348

TransUnion LLC, P.O. Box 2000, Chester, PA 19022

PROTECT YOUR PRIVACY: ADDITIONAL IDENTITY THEFT PREVENTION TIPS

Opt out of pre-screened credit card offers:

- Call 888-5-OPT-OUT (888-567-8688)
- Visit <https://www.OptOutPreScreen.com/>

Opt out of junk mail:

- Visit <https://www.DMAChoice.org/>

Shred your documents. If you do not own or have access to a shredder, look for community shred events that offer this service free of charge.

Use a locking mailbox to prevent mail theft.

Use a safe or locking file drawer to secure personal information in your home.

Don't carry sensitive information in your purse or wallet, unless it is necessary. You should leave your Social Security card, bank account PIN, insurance cards and other important documents in a secure place.

Make copies of important documents, including your credit cards (front and back), Social Security card and insurance cards. If your purse or wallet is stolen, you will have all the information easily accessible if you need to replace cards or close 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 agencies. If you have a membership card that uses your SSN, ask for a randomly generated ID number instead.

Be wary of email scams:

- Financial institutions never ask for personal info by email.
- Scammers will use many tactics to trick you into sending them your personal information, or clicking on a link containing a virus.
- Delete any suspicious messages immediately and be cautious of emails that include attachments. You may also forward suspicious emails to spam@uce.gov.
- Don't access sensitive information online unless you know the connection is secure.

Websites that protect your informa-

tion with encryption have “https” at the beginning of the web address (the “s” represents a secure connection).

- Use strong passwords and PIN numbers for your credit card, bank, and utility accounts and any other website that requires log-in information.
- Be mindful of what you post on social media, as it can lead to unintended consequences. Hackers or scammers can use social media postings to compromise other online accounts.



THE MANY FORMS OF IDENTITY THEFT

NEW ACCOUNT FRAUD



Someone opens a new credit card or bank account, enrolls with a utility provider, obtains loans or makes other credit purchases using your name and/or other stolen personal information, such as your address, date of birth or Social Security Number. When the bills aren't paid, creditors and possibly debt collectors come after you. Victims may not be immediately aware of the fraud, as account statements are routed to an address used by the imposter.

EXISTING ACCOUNT FRAUD

Someone acquires your credit information or gains access to your bank or utility account and makes unauthorized purchases or withdrawals. Victims may not discover this until receiving and reviewing their account statement.

Under federal law, you are afforded more protection for your credit cards than your ATM or debit cards. Accordingly, it is advisable to use a credit card for online purchases.

You have 60 days to report fraudulent credit card charges. If you do so, the credit card company cannot hold you liable for more than \$50 worth of the disputed charges.

If your debit card is used for fraudulent transactions and you report it within **two business days**, you are liable for up to \$50. If you report it between two days and 60 days after the incident, you are liable for up to \$500. If you do not notice and report the problem within 60 days, you could be responsible for all unauthorized charges.

PayPal and other online escrow services may have varying fraud recovery provisions. You should read the company's user agreement before signing up for more information on security and privacy measures taken to protect your information. For instance, PayPal will not hold you liable if you report a fraudulent charge within 60 days.

STOLEN CHECKS AND FRAUDULENT BANK ACCOUNTS

Someone has stolen your checks or has written counterfeit checks on your account. You should immediately notify your bank and request a fraud affidavit. Stop payment on the checks, close the compromised accounts and have the bank notify the check verification service with which it does business so that retailers will be alerted not to accept those checks. If your checks have been stolen and you know where the thief has used them, contact the verification company that the merchant uses. Some of the major ones are:



- ChexSystems: 800-428-9623, <https://www.consumerdebit.com>
- Certegy, Inc.: 800-237-3826, <https://www.askcertegy.com/checkMain.jsp>
- TeleCheck: 800-710-9898, <http://www.firstdata.com/telecheck/>
- CrossCheck: 800-843-0760, <http://www.cross-check.com/>

FRAUDULENT CHANGE OF ADDRESS

Someone has filed a change of your address with the post office or has used the mail to commit credit or bank fraud. Notify the U.S. Postal Inspection Service at 410-715-7732.

SOCIAL SECURITY NUMBER MISUSE



Someone has gotten hold of your Social Security Number to fraudulently obtain Social Security benefits or has used it in concert with other personal information to seize your identity for illicit means. Contact the

Identity Theft Unit at 410-576-6491 or the Federal Trade Commission at 877-438-4338 for information or advice on how to resolve the issue

DRIVER'S LICENSE NUMBER MISUSE

Similar to Social Security Number misuse, this is when someone has gained access to your driver's license number and has used it as identification to pass bad checks. Call the Maryland Motor Vehicle Administration at 800-950-1682 to see if you are eligible to be issued a new

number. You can also find out if a replacement license has been issued in your name and ask to have a fraud alert put on your license.

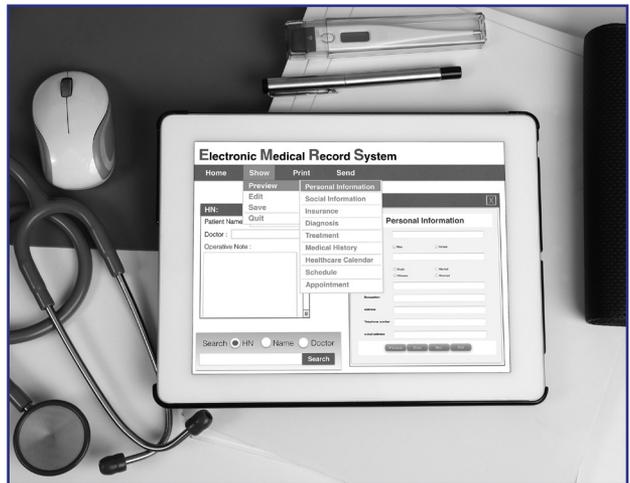
CRIMINAL IDENTITY THEFT

Someone fraudulently uses your personal information in the commission of a crime. Sometimes, identity theft victims learn that imposters using their name were arrested or had arrest warrants issued against them. If criminal violations are wrongfully issued in your name, contact the police department that arrested the person using your identity or the court that issued the arrest warrant. You may need to file an impersonation report to confirm that this is a case of misidentification.

Clearing your name of wrongful criminal records can be challenging. The Privacy Rights Clearinghouse (<http://www.privacyrights.org/>) has a helpful fact sheet to guide you through this process.

MEDICAL IDENTITY THEFT

Someone uses your personal, health or insurance information to obtain health care or medical products, or to submit false claims to an insurer for medical treatments you never sought or received. This may result in erroneous entries in an existing medical record or the creation of false medical records in the victim's name. The consequences for this type



of identity fraud can be life-threatening. For example, if an identity theft victim is unconscious and needs emergency treatment, the victim's medical record may contain inaccurate information about a patient's blood type, allergies, medication or other medical conditions that could be fatal.



TAX FRAUD

Someone uses your Social Security Number or personal information to fraudulently file a tax return. This often causes the government to

mistakenly issue a refund to the fraudster. As a result, when you file your tax returns, they may be rejected or you may receive written notification from the IRS indicating a problem with your filing.

The IRS will never call or email taxpayers to ask for money or personal information, nor will they threaten consumers over the phone with arrest, deportation or other penalties. The IRS will also never ask taxpayers to wire money or use a prepaid debit card to file their returns.

In 2014, tax-related identity theft was the most common form of identity theft reported to the Federal Trade Commission and other consumer and law enforcement agencies.

If you suspect that you're a victim of tax fraud, please contact:

- The Internal Revenue Service Identity Protection Specialized Unit at 800-908-4490.
- The Comptroller of Maryland Questionable Return Team at 410-260-7449.

TAKE ACTION: WHAT TO DO IF IT HAPPENS TO YOU

IDENTITY THEFT RECOVERY CHECKLIST

- Place fraud alert and obtain credit report
- Report crime to police
- Dispute and close fraudulent accounts
- Report incident to the Federal Trade Commission
- Keep detailed records of all communications related to the incident
- Consider placing a credit freeze on credit reports (see “Consider A Credit Freeze,” page 7)
- Consider submitting identity theft passport application (see “Identity Theft Passport”, page 20)

PLACE AN INITIAL FRAUD ALERT

When you first become aware of an identity theft incident, you should immediately place a fraud alert on your credit report and request a copy of your credit report by calling one of the three credit

reporting agencies (whichever agency you call is required by law to notify the other two). A fraud alert lasts 90 days and can be renewed by calling any of the credit reporting agencies again. Review your credit report for any unusual activity, especially accounts in bad standing. Many times your credit report is the only way to detect fraudulently opened accounts.

To place a fraud alert:

Equifax

888-766-0008

<https://www.alerts.equifax.com>

Experian

888-397-3742

<https://www.experian.com/fraud/center.html>

TransUnion

800-680-7289

<http://www.transunion.com/fraud>

REPORT CRIME TO POLICE

You should also report the incident to your local law enforcement agency. State law requires police to take a report of identity theft and give you a copy, regardless of where the crime occurred.

CONTACT THE FTC

Report the fraud to the Federal Trade Commission at www.ftc.gov/idtheft or by calling 877-438-4338. The agency has additional resources to assist identity theft victims.

DISPUTE AND CLOSE FRAUDULENT ACCOUNTS

Many businesses have established policies and procedures for dealing

MD. CODE, CRIMINAL LAW ARTICLE SECTION 8-304

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

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

with identity theft victims. If you have trouble closing fraudulent accounts, disputing charges on existing accounts or need sample dispute letters, contact the Office of the Attorney General Identity Theft Unit.

Write to collection agencies that are demanding payment and inform them that you are a victim of fraud and are not responsible for the payments. Include a copy of your police report, an identity theft affidavit that you may have filled out and any other supporting documents.

IDENTITY THEFT PASSPORT

The Identity Theft passport is a tool that may help you resolve financial issues caused by identity theft, and to help prevent a wrongful arrest if a thief uses your personal information during the commission of a crime. To learn more or to obtain an application, go to <http://www.oag.state.md.us/idtheft/IDTpassport.htm>.

DATA BREACHES: REDUCE YOUR RISK

DATA BREACH RESPONSE CHECKLIST

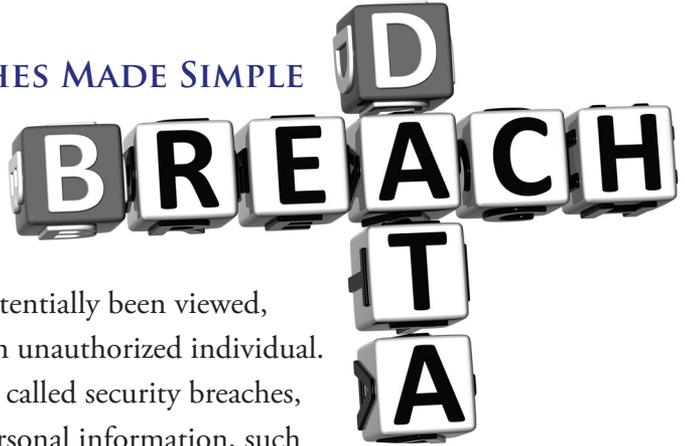
- Place fraud alert and obtain credit report
- Determine what data may have been compromised and act accordingly
- Make appropriate changes to potentially impacted data (e.g. cancel cards, change passwords, close accounts)
- Take advantage of any free credit monitoring offers provided by the affected business
- Keep detailed records of all communications related to the incident
- Consider placing a credit freeze on credit reports (see “Consider A Credit Freeze,” page 7)
- Contact the Maryland Office of the Attorney General or the Federal Trade Commission for additional identity theft information

DATA BREACHES MADE SIMPLE

A data breach occurs when sensitive or confidential

information has potentially been viewed, stolen or used by an unauthorized individual.

Data breaches, also called security breaches, can expose your personal information, such as Social Security Numbers, financial account information, user names and passwords, medical records and more.



A data breach can occur when a company's website is hacked, a computer is stolen, data tapes or other records are lost in the mail or through inadvertent disclosure of private information.

The Maryland Personal Information Protection Act requires any business that keeps electronic records containing the personal information of Maryland residents to notify those residents if their information is compromised. The business must also provide notice to the Office of the Attorney General. This enables Marylanders to protect themselves from fraud and identity theft.

The business sending the data breach notice will often offer complementary credit monitoring services. Consider taking advantage of the offer if, upon review, you think it will be beneficial. Contact the company extending the offer, the credit monitoring agency or the Office of the Attorney General Identity Theft Unit if you have additional questions about credit monitoring services.

To further minimize the risk of identity theft following a data breach, you should consider making changes to the affected accounts. That may include changing user names, passwords and requesting new credit or debit card account numbers.

ADDITIONAL RESOURCES

Federal Trade Commission

The FTC offers a universal fraud affidavit and an in-depth guide for recovering from identity theft. Victims can also file a complaint with the FTC that may help law enforcement investigate and prosecute identity thieves.

<http://www.consumer.gov/idtheft>

877-ID-THEFT (438-4338)

Privacy Rights Clearinghouse

The Privacy Rights Clearinghouse is a nonprofit organization that educates and empowers individuals to protect their privacy while communicating trends to policymakers, industry and media.

<http://www.privacyrights.org>

619-298-3396

Identity Theft Resource Center

The Identity Theft Resource Center is a nonprofit organization dedicated to the understanding and prevention of identity theft.

<http://www.idtheftcenter.org>

888-400-5530 ext 103

Maryland State Bar Association

The Maryland State Bar Association may be able to help you find an attorney if you wish to pursue legal action against someone who allegedly stole your identity.

<http://www.msba.org/>

410-685-7878

FOR MORE INFORMATION AND ASSISTANCE, CONTACT:

Maryland Office of the Attorney General Identity Theft Unit

200 St. Paul Place

Baltimore, MD 21202

410-576-6491

410-576-6566 (Fax)

IDTheft@oag.state.md.us

www.marylandattorneygeneral.gov/Pages/IdentityTheft/



BRIAN E. FROSH
ATTORNEY GENERAL

MARYLAND OFFICE OF THE ATTORNEY GENERAL
410-576-6300
1-888-743-0023 TOLL-FREE
TDD: 410-576-6372

200 ST. PAUL PLACE, BALTIMORE, MD 21202

WWW.MARYLANDATTORNEYGENERAL.GOV