Identity Theft:

Protect Yourself, Secure Your Future

Consumer Protection Division
Maryland Office of the Attorney General

June 2020

Identity Theft:
Protect Yourself, Secure Your Future

In our fast-paced digital world, it's never been more important to protect your personal information. If your Social Security number, health records, bank accounts, financial information, PINS and passwords, or other data falls into the wrong hands, the damage can be swift, severe, and long-lasting.

Unfortunately, identity theft has become an all-too-common occurrence, impacting millions of Americans every year. Your identity can be stolen by anonymous computer hackers half a world away or by someone you know and trust.

The Maryland Office of the Attorney General Identity Theft Unit produced this guide to empower you to take a more active role in protecting your identity and to provide you with helpful information and resources to recover from identity theft if it happens to you.

Brian E. Frosh

Maryland Attorney General

Identity Theft:

Protect Yourself, Secure Your Future

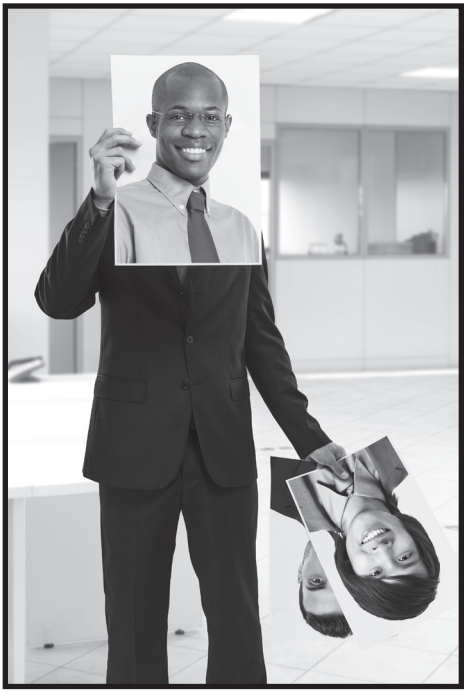
Contents

Maryland Office of the Attorney General
Consumer Protection Division
Identity Theft Unit

What Is Identity Theft?

Identity theft occurs when someone uses your personal information to:

- Purchase goods, property, or services without your consent;
- Create fake financial accounts in your name;
- Impersonate you for financial gain or to receive medical care;
- File fraudulent tax returns under your name to obtain your refund; and/or
- Commit other crimes that can damage your personal credit and reputation.



Identity theft is one of the fastest growing crimes in the country, affecting over 15 million Americans each year. Victims often spend hundreds of hours and thousands of dollars to fix the damage caused by identity thieves.

This booklet will help you learn what identity theft looks like and how it happens, how to reduce your risk of identity theft, and give you specific guidance to help recover if your identity is stolen. Look for this symbol for quick tips to help avoid identity theft.

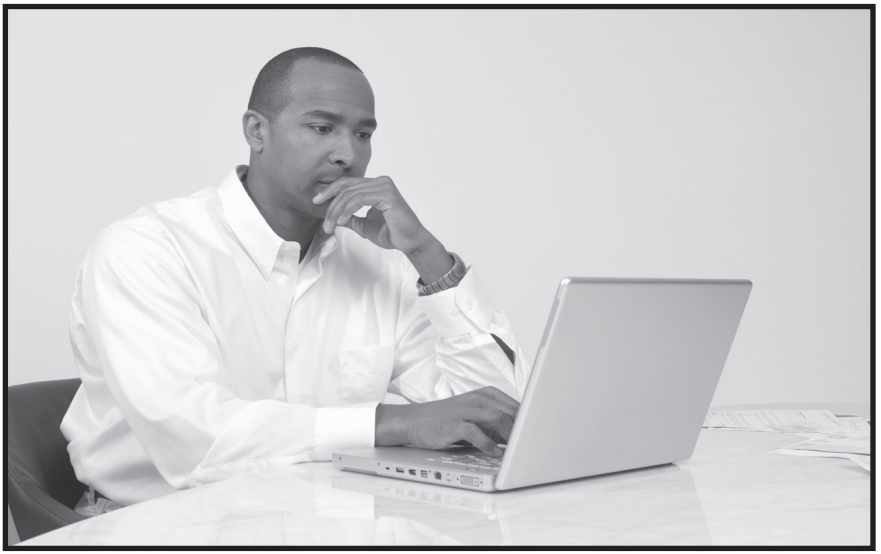
What Does Identity Theft Look Like?

Identity theft can take many forms. Often, identity thieves like to

simply steal money. This is called **financial identity theft**. Financial identity theft generally takes one of two forms: **existing account fraud** or **new account fraud**.

Existing account fraud is extremely common, and there is a good chance you have already experienced it at some point in your life. This type of fraud happens when an identity thief gains access to an account that you created. For example, if an identity thief makes a purchase using your stolen credit card number, you are a victim of existing account fraud. **Existing account fraud can be relatively easy to spot, but difficult to prevent.**

Diligently monitoring your account statements for unauthorized activity is one of the best ways to spot existing account fraud. Be sure to check your account statements at least once a month, but more frequently if possible.



New account fraud occurs when identity thieves use stolen information to create a new account in your name. By using your stolen information (name, date of birth, or Social Security number, for

example), someone may be able to open a credit card or utility account in your name. This type of fraud can be very dangerous because it may go undiscovered for many years. Victims often discover the new accounts when they are contacted by a debt collection agency or applying for credit.

New account fraud can be hard to spot, but it's easy to prevent. A free tool, called a **credit freeze** is extremely effective at preventing new account fraud. For more information about credit freeze, see page 13. Checking your credit report annually from each of the three major credit reporting agencies is a good way to see if an identity thief has fraudulently opened an account in your name. The three major credit reporting agencies are Equifax, Experian, and TransUnion. See page 17 for instructions on checking your credit reports.

Check your credit report from all three major credit reporting agencies at least once per year. Also consider placing a credit freeze with all three credit reporting agencies before identity theft happens. This is one of the only preventative tools in the world of identity theft.

Other common forms of identity theft include medical, criminal, and income tax fraud.

- **Medical identity theft** occurs when an unauthorized person uses your personal information to receive medical care. This is dangerous because it could negatively affect your insurance rates, or potentially lead to an inaccurate diagnosis or dangerous drug interaction.
- **"Criminal" identity theft** occurs when a person uses your personal information in the commission of a crime, often as an alias or during a traffic stop.
- **Income tax identity theft** occurs when a person uses your personal information to file a fraudulent tax return to obtain a tax refund. The identity thief will submit phony tax information to receive a large tax refund in your name.

Identity thieves seem to be endlessly inventive. As a result, the list of miscellaneous forms of identity theft is ever-growing. If identity thieves can find a way to benefit from using your stolen information, they will. Common examples include **government benefits, Social Security payments, jobs, apartment rentals, student loans, utility accounts,** and much more.

How Does Identity Theft Happen?

Identity theft happens when identity thieves obtain your personal information. They can do this in one of three ways: they steal it, obtain it from publicly shared social media, or trick you into giving it away.

Identity thieves can steal information in many ways. Some methods, like physically stealing your wallet or purse, don't rely on technology. Physically stealing your information can limit identity thieves to a particular location or a limited number of stolen files. Other methods, such as hacking into your email or a business database can happen from anywhere in the world using sophisticated technology. Stealing data from a government or business database is sometimes called a "**data breach**." Data breaches can allow a single person to steal a massive amount of information. For more information on data breaches, see page 6.

Consider that what you post on social media sites is visible to many people, not necessarily just your close friends. Be cautious about posting information (like your birthday or birthplace) that could help an imposter steal your identity.

Identity thieves can also use information that you gave away. Be mindful about what you publicly post on social media because identity thieves can search out useful information even if you think it's harmless to share. For example, it may seem harmless to post your birthday on a social media site, but thieves can use this information with other information about you to steal your identity. More commonly, however, identity thieves use **fraud** to trick you into giving away private information. Some of the most common ways to trick you into giving away valuable information are scams called "phishing" and "imposter fraud." More information about these and other types of scams is available on the Maryland Attorney General's website, www.marylandattorneygeneral.gov, by clicking on Services, and then Consumer Protection.

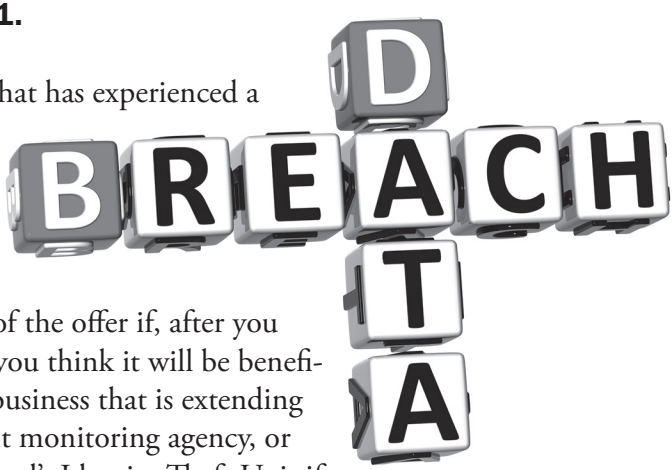
What Are Data Breaches?

A data breach occurs when sensitive or confidential information has been accessed, 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 business's website is hacked, a computer is stolen, data tapes or other records are lost in the mail, or through an unintentional release of private information. The Maryland Personal Information Protection Act (PIPA) 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 them-

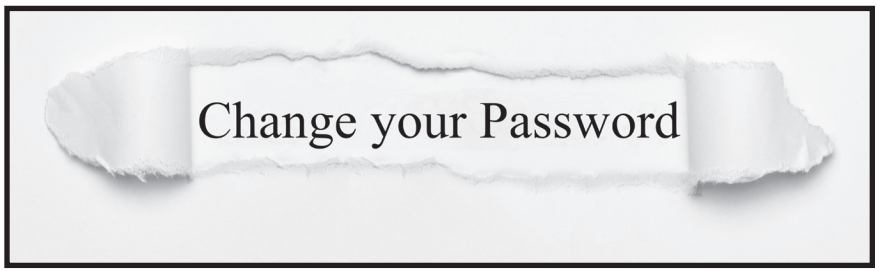
selves from fraud and identity theft. These notices are posted on the Attorney General's website under "Security Breach Notices," and are searchable by the business's name.

Take it seriously if you receive a notice from a business that they have experienced a data breach and your personal information may be at risk of being exposed or stolen. If you have any questions about the authenticity of the notice, reach out to the Attorney General's Identity Theft Unit at IDTheft@oag.state.md.us or 410-576-6491.



Often a business that has experienced a data breach will offer complementary credit monitoring services. Consider taking advantage of the offer if, after you review its details, you think it will be beneficial. Contact the business that is extending the offer, the credit monitoring agency, or the Attorney General's Identity Theft Unit if you have additional questions about credit monitoring services.

To further minimize the risk of identity theft following a data breach, consider changing your user name and password and, if the breach involved a bank or other creditor, requesting new credit or debit card account numbers.

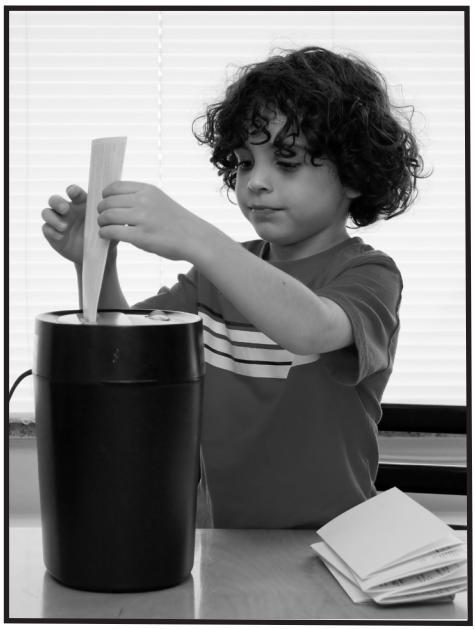


If you have received a data breach notice, use this checklist to help reduce your risk of becoming a victim of identity theft.

- ❑ Place a fraud alert with each of the three major credit reporting agencies (page 15).
- ❑ Obtain a copy of your credit report from each of the three major credit reporting agencies (page 17).
- ❑ Make appropriate changes to your impacted information (change passwords, cancel cards, or close accounts, for example).
- ❑ 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 your credit reports (page 18).

How Can I Avoid Becoming a Victim?

You can't *eliminate* the risk of identity theft. However, you can reduce your risk by taking certain steps to protect your private information.



Protecting Yourself at Home

Although identity thieves can strike from the other side of the world, it's important to secure information in your own home, because it's likely where you spend most of your time and keep many of your **sensitive documents**. Some identity thieves know or have a relationship with their victim. For example, party guests or neighbors may be able to physically steal documents from you that are left unse-

cured. Mobile smartphones with cameras eliminate the need to actually steal your documents—the identity thief can simply capture the information in a quick photograph. Follow these tips to help protect your information at home.

- Shred sensitive documents you no longer need, such as credit card offers, financial statements, and medical documents;
- Use a locking mailbox;
- Use a safe or locked file storage system to protect sensitive documents;
- Opt out of pre-screened credit card offers by calling 1-888-5-OPT-OUT (1-888-567-8688) or visiting www.OptOutPreScreen.com; and
- Opt out of "bulk" mail by visiting www.DMAChoice.org.

Keep your sensitive documents in a locked, secure location in your home. Thieves no longer need to physically steal your paperwork—they can just take a photo of it with a smart device, like a phone or tablet.

Protecting Yourself on the Go

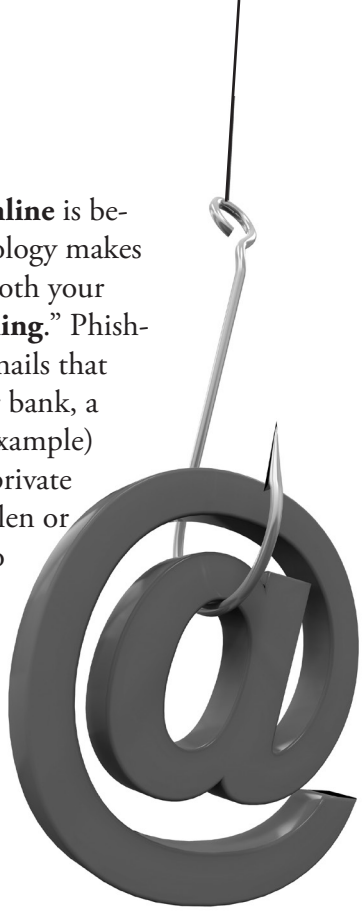
It's easy to accidentally—and unnecessarily—carry sensitive information in your purse or wallet. Unless you specifically need the information for a job interview or an appointment, you should leave your Social Security card, bank account PIN, insurance cards, and other important documents in a secure place at home. You may also want to **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 at home if you need to replace cards or close your accounts.

Don't give out your Social Security number unless it's absolutely necessary. Sometimes you will be required to use your Social Security number for tax purposes, Medicare, or to request a credit report from a credit agency. If you have a membership card that uses your Social Security number, ask for a randomly generated identification number

instead.

Protecting Yourself Online

Protecting your sensitive information **online** is becoming more and more difficult. Technology makes it very easy for identity thieves to steal both your money and information through "**phishing**." Phishing occurs when identity thieves send emails that appear to be from a trusted source (your bank, a utility service provider, or a friend, for example) in an effort to trick you into providing private information. Often, these emails use stolen or counterfeit graphics, and may ask you to "confirm" a password or other sensitive account information, enter payment information, or open an attachment. Keep these tips in mind to protect your information online:



- Financial institutions never ask for personal information by email;
- Don't click on links in unfamiliar emails. Those links can contain a virus or malicious software that can infect your computer; and
- Delete any suspicious emails immediately.

A Note About Passwords

It's nearly impossible to keep track of all the unique passwords we use online, so here are a few ways to keep your accounts more secure.

Consider using multi-factor authentication (MFA), which requires your password AND an additional piece of information to access the account. Usually the additional piece of information is a short code sent to a smartphone, email, or other trusted device. Even if someone is able to successfully guess your password, they will be unable to access your account unless they also have the second piece of informa-

tion required.
Do NOT use the same password for multiple sites! If one website is hacked, and the identity thieves learn your password, they may be able use it on other accounts if you reuse the same passwords.

Write down clues or reminders rather than your actual passwords if you have trouble remembering them. Compare the following reminder phrases like "my third dog and dad's birth year" versus "Spot1950." One will be meaningful to you, but meaningless to someone who may view the written clue.

Consider using fake answers for password recovery questions. If you have ever forgotten your password, you know that many online accounts will ask you a series of questions to recover your password. If you have a prominent social media presence, or you suspect an identity thief knows a lot about you, you can use nonsense answers for your recovery question. For example, "Where did you grow up?" is a common recovery question. Many people that know you or have access to your personal information may be able to accurately answer that question. However, if you put something that's clearly not true ("The Moon," for example), it will be much harder for an identity thief to compromise your account.

What Are Credit Reports?

There are three major nationwide credit reporting agencies: Equifax, Experian, and TransUnion. Credit reporting agencies collect and maintain information about consumers and their financial history in something called a "credit report." Credit reports are used to generate something called a "credit score," which is often used by lenders and creditors to decide whether to provide you with a service and if so, on what terms (for example, interest rates). Generally, a better credit score results in more access to lender and creditor services, and on more favorable terms.

While a credit score is important, the underlying information on a credit report is what determines a credit score. Therefore, it's impor-

tant that your credit report is accurate and free from fraud. 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 have filed for bankruptcy.

If you are a Maryland resident, you can receive up to six free credit reports each year. Federal law entitles you to one free report from each credit reporting agency each year, and Maryland law entitles you to an additional free report from each credit reporting agency each year.

You may request a free copy of your credit report from each of the three major credit reporting agencies once a year. This is one of the easiest and most effective ways to see if you are a victim of identity theft, specifically **new account fraud** (page 3). 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. You can also obtain free credit reports through Annual Credit Report, an organization authorized by federal law to provide credit reports from Equifax, Experian, and TransUnion. See page 17 for

instructions on obtaining your credit reports.

How to Protect Your Credit Report

You can completely block the information on your credit report from would-be creditors or lenders through a credit "freeze." Freezing your credit report is one of the only ways to help **prevent** identity theft. If you have a credit freeze in place, any new account opened in your name **must get your approval**. In other words, you are the one who decides what accounts can be opened in your name, rather than a creditor or lender making that decision.

Most businesses will not open credit accounts without first checking a consumer's credit history through a credit report. Even someone who has your name and Social Security number might not be able to get credit in your name if your credit reports are frozen. You can freeze your credit reports at no cost.

While a credit freeze can help protect against identity theft, it may not be for everyone. If you plan to apply for a credit card or to rent an apartment in the near future, it's likely that your credit report will need to be accessed and you will need to lift the freeze (this also called a "thaw").

You can also freeze the credit of a minor dependent, which can help protect them against fraud and identity theft.

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 they turn 18. When parents or guard-

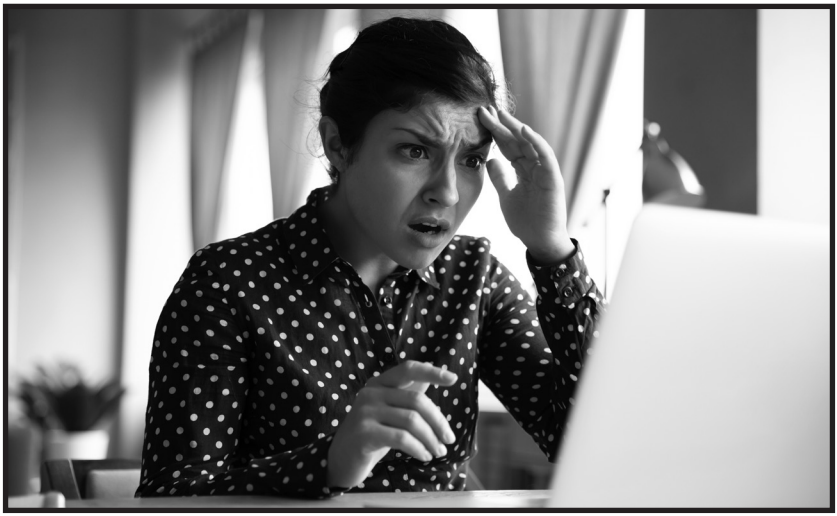
ians take advantage of this opportunity, they can ensure a child will begin their adult life with a clear credit history. This law extends protection to other consumers who meet certain eligibility requirements. Contact the Attorney General's Identity Theft Unit at 410-576-6491 to find out who may be eligible for this protection.

To place a credit freeze for your child, a parent or guardian must submit this information 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

I Think My Identity Has Been Stolen—What Can I Do?



If any of the following have happened, you may be a victim of identity theft:

- Your bank or credit card statements never arrive in the mail;
- You receive acknowledgments of new accounts opened that you don't recognize;
- You receive calls from collection agencies demanding payment for accounts you never opened or purchases you never made;
- There are mysterious charges on your credit card bill;
- Accounts that you didn't open appear on your credit reports;
- There are excessive credit inquiries or any unfamiliar activity on your credit reports;
- You are denied credit or offered less favorable credit terms, such as high interest rates; or
- Law enforcement has warrants for a crime committed in your name.

Treat any unfamiliar activity in your account statements, credit reports, or mail as suspicious. Don't assume the unfamiliar activity is an error and will go away on its own.

Identity Theft Recovery Steps

If you are—or think you may be—a victim of identity theft, **follow these six steps** for the best chance of recovering your financial standing.

Keep detailed records of your identity theft resolution process. Disputing identity theft can take weeks or months, and it's easy to lose track of with whom you spoke or what information they gave you.

1 Place a Fraud Alert on Your Credit Reports

(Please note: this is not the same thing as a "credit freeze")

When you first become aware that you may be the victim of identity theft, 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 (see contact information, below). Whichever agency you call is required by law to notify the other two. A fraud alert lasts for one year, and can be renewed by calling any of the credit reporting agencies. Review your credit report for any unusual activity, especially accounts in bad standing. Often your credit report is the only way to detect accounts in your name that were opened fraudulently.

Equifax
888-766-0008
www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

Experian
888-397-3742
www.experian.com/fraud/center.html

TransUnion
800-680-7289
www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page

2 Report the Crime to Police

Report the crime to your local law enforcement agency. Maryland law requires your local police to take a report of identity theft and give you a copy regardless of where in the world the crime occurred (Md. Code, Criminal Law, Article §8-304).

3 Get Free 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 have filed for bankruptcy. 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. 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; Maryland residents may request one additional report each year at no cost. This is one of the easiest and most effective ways to prevent identity theft.

There are three ways to request your credit reports:

- Phone: 1-877-322-8228
- Online: www.annualcreditreport.com
- Mail: See attached form on page 21.

Note: Through April 2021, three nationwide credit reporting agencies—Equifax, Experian and TransUnion—are offering free weekly online credit reports. The free weekly credit reports are only available through www.annualcreditreport.com.

4 Contact the Federal Trade Commission

Report the fraud to the Federal Trade Commission by calling 1-877-438-4338 or go online to www.identitytheft.gov. You can compile a record of what happened in a central document, called an Identity Theft Report, through this site. The report can be useful when disputing fraudulent accounts or charges (see the sample dispute letter on page 22).

5 Dispute Fraudulent Accounts

Many businesses have established policies and procedures for dealing with identity theft victims. If you have trouble closing fraudulent accounts, disputing charges on existing accounts, or need sample dispute letters, contact the Attorney General's 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.

See page 22 for a sample dispute letter that you can use as a template.

6 Consider a Credit Freeze

(Please note: this is not the same thing as a "fraud alert")

A credit freeze (sometimes called a security freeze) 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. You can freeze and thaw your credit reports at **no cost**.

If you decide to obtain a credit freeze, you will need to contact **each** of the credit reporting agencies.

Equifax

- Phone: 1-888-298-0045
- Online: www.equifax.com/personal/credit-report-services
- Mail: Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348

Experian

- Phone: 1-888-397-3742
- Online: www.experian.com/freeze/center.html
- Mail: Experian Security Freeze, P.O. Box 9554, Allen, TX 75013

TransUnion

- Phone: 1-888-909-8872
- Online: www.transunion.com/credit-freeze
- Mail: TransUnion LLC, P.O. Box 2000, Chester, PA 19022

If you are requesting a credit freeze by mail, you will need to include all of this information:

- Your full name, address, Social Security number, and date of birth;
- Prior addresses and proof of prior names, if you have moved or had a name change in the past five years;
- A copy of a government-issued ID card; and
- A copy of a bank statement or utility bill confirming your current address.

Other Forms of Identity Theft

There are additional steps you can take to help recover if any of the following forms of identity theft happen to you.

Tax Fraud

- Federal: Contact the Internal Revenue Service Identity Protection Specialized Unit at 1-800-908-4490.
- Maryland: Contact the Questionable Return Team at the Maryland Office of the Comptroller at 410-260-7449.

Student Loans

- Contact the school that opened the loan and explain that you are a victim of identity theft. Ask to close the loan and follow their instructions on what they will need from you to dispute the loan.
- If the fraudulent loan is a federal student loan, contact the U.S. Department of Education Office of Inspector General hotline at 1-800-MISUSED (1-800-647-8733) or the U.S. Department of Education Federal Student Aid Ombudsman at 1-877-557-2575.

Checking Accounts

- Order a free copy of your ChexSystems report, which compiles information about your checking accounts. To get your ChexSystems report, call 1-800-428-9623.
- If someone is writing bad checks against your account, contact your financial institution. Report the stolen checks, close your account, and ask your financial institution to report the fraud to the check verification system.
- Contact check verification companies Telecheck (1-800-710-9898) and Certegy (1-800-237-3826). Report that your checks were stolen and ask them to tell businesses to refuse the stolen checks.

Tools

Additional Resources

Annual Credit Report Request Form

You have the right to get a free copy of your credit file disclosure, commonly called a credit report, once every 12 months, from each of the nationwide consumer credit reporting companies, Equifax, Experian and TransUnion.

For instant access to your free credit report, visit www.annualcreditreport.com.

For more information on obtaining your free credit report, visit www.annualcreditreport.com or call 877-322-8228.

Use this form if you prefer to write to request your credit report from any, or all, of the nationwide consumer credit reporting companies. The following information is required to process your request. **Omission of any information may delay your request.**

Once complete, fold (do not staple or tape), place into a #10 envelope, affix required postage and mail to:
Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281.

Please use a Black or Blue Pen and write your responses in PRINTED CAPITAL LETTERS without touching the sides of the boxes like the examples listed below:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

Social Security Number: ___ - ___ - ____

Date of Birth: ___ / ___ / ____
Month / Day / Year

Fold Here — Fold Here

First Name _____ **M.I.** _____

Last Name _____ **JR, SR, III, etc.** _____

Current Mailing Address:

House Number _____ **Street Name** _____

Apartment Number / Private Mailbox _____ **For Puerto Rico Only: Print Urbanization Name** _____

City _____ **State** _____ **ZipCode** _____

Previous Mailing Address (complete only if at current mailing address for less than two years):

House Number _____ **Street Name** _____

Fold Here — Fold Here

Apartment Number / Private Mailbox _____ **For Puerto Rico Only: Print Urbanization Name** _____

City _____ **State** _____ **ZipCode** _____

Shade Circle Like This → ●

Not Like This → ⊗ ✓

I want a credit report from (shade each that you would like to receive):

- ○ Equifax
- ○ Experian
- ○ TransUnion

○ **Shade here if, for security reasons, you want your credit report to include no more than the last four digits of your Social Security Number.**

If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

31238

Sample Dispute Letter

[Date]

[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Name of Company]
[Fraud Department]
[Address]
[City, State, Zip Code]

[RE: Your Account Number (if known)]

Dear [Name of Company]:

I am a victim of identity theft. I recently learned that my personal information was used to open an account at your company. I did not open or authorize this account, and I request that it be closed immediately. Please send me written confirmation that I am not responsible for charges on this account, and take appropriate steps to remove information about this account from my credit files.

I have enclosed a copy of my Identity Theft Report and proof of my identity. I also have enclosed a copy of my police report. When you receive a request like this with an Identity Theft Report, you must stop reporting fraudulent debts to credit bureaus.

Please send me a letter explaining your findings and actions.

Sincerely,
[Your Name]

Enclosures: [List what you are enclosing] • Identity Theft Report • Proof of Identity [a copy of your driver's license or state ID] • Police Report

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.
- ☐ Keep sensitive documents in a locked, secure location.
- ☐ Shred documents containing personal information that you no longer need.
- ☐ Be very suspicious of unexpected calls from someone demanding money or personal information.
- ☐ Don't post information online that could help an imposter steal your identity.
- ☐ Keep your computer's virus protection software up-to-date.

Notes

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