ANTHONY G. BROWN
Attorney General

Candace McLaren Lanham
Chief of Staff

CAROLYN QUATROCKI
Deputy Attorney General

WILLIAM D. GRUHN
Chief

Consumer Protection Division

STATE OF MARYLAND
OFFICE OF THE ATTORNEY GENERAL
CONSUMER PROTECTION DIVISION

Identity Theft Recovery and Prevention Information

*****Are you a victim of identity theft? If so, have you completed the following checklist?*****

- ☐ Place fraud alert and obtain credit report
- ☐ Report identity theft to the Federal Trade Commission
- ☐ Dispute and close disputed accounts
- ☐ Report crime to police
- ☐ Consider placing a credit freeze on credit reports

Remember to keep detailed records of all communications related to the incident!

The Identity Theft Program will be able to help you by giving you advice and materials that can make the recovery and/or prevention process easier for you. Follow these steps first, if you have any questions, feel free to contact:

Jeff Karberg, Director
Maryland Attorney General Identity Theft Program
Address: 200 St. Paul Place Baltimore, MD 21202
Phone: 410-576-6491
Fax: 410-576-6566
Email: IDTheft@oag.state.md.us
http://www.marylandattorneygeneral.gov

*****Info on how to complete your checklist starts on the next page*****

1. Place a Fraud Alert (Please note: this is not the same thing as a "credit freeze")

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 for one year 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.

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

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

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

2. 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'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. 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. This is one of the easiest and most effective ways to prevent identity theft.

How to request your free credit report:

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

3. Contact the Federal Trade Commission

Report the fraud to the Federal Trade Commission by calling 1-877-438-4338 or go online to https://www.identitytheft.gov

4. 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 Identity Theft Program.

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.

5. Report Crime to Police

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

Maryland Criminal Law 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.

6. Consider a Credit Freeze (Please note: it's not the same thing as a "fraud alert")

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. **You can freeze your 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 lift the freeze.

7. Obtain a Credit Freeze

(Note: You'll need to contact each of the three credit reporting agencies)

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:

- Full name, address, Social Security Number and date of birth;
- 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.

8. 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 extends protection to consumers who meet certain eligibility requirements. 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

9. Identity Theft and 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 Comptroller's Office at 1-410-260-7449.

10. 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 at home.

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 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 information 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. Fox example, hackers or scammers can use social media postings to compromise other online accounts.

11. Data Breach Response Checklist

- ☐ Place fraud alert and obtain credit report
- ☐ Determine what data may have been compromised 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 3)
- ☐ 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.

Often times, the business sending the data breach will offer complementary credit monitoring services. Consider taking advantage of the offer if, after 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.

12. 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 Sir or Madam:

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