Consumer Alert: Beware of Door-to-Door COVID-19 Testing

The Maryland Office of the Attorney General is alerting Marylanders of individuals and labs offering door-to-door COVID testing. The individuals performing these tests promise prompt results but consumers have reported not receiving results several weeks after the initial test. Consumers have complained that they do not know how their personal identifying information is being secured.

Consumers are advised to only get tested at approved COVID-19 testing sites. Visit covidtest.maryland.gov for a list of approved COVID-19 testing sites in Maryland. Your local health department can also provide information about testing in your area. Consumers should avoid testing conducted by random strangers who show up at their doors.

As of January 15, 2022, and during the public health emergency, private health insurance covers the cost of most over-the-counter COVID tests. Also, consumers can now request and receive four tests per household from the federal government at no cost. There are no shipping costs, and you don't have to provide a credit card or bank account number. You only need to provide a name and address. Anyone who asks for more information than that is likely a scammer. So, remember:

- Visit COVIDtests.gov or call 1-800-232-0233 (TTY 1-888-720-7489) to order your free COVID test kits from the federal government. If you order online, you'll be redirected to special.usps.com/testkits. If you follow a link from a news story, double-check the URL that shows in your browser's address bar.
- No one will call, text, or email you from the federal government to ask for your information to "help" you order free kits. Only a scammer will contact you, asking for information like your credit card, bank account, or Social Security number. Do not respond. Instead, report it to the FTC at ReportFraud.ftc.gov.

"We are monitoring these activities, but consumers should be on the alert and are urged to protect themselves against identity theft and scams by only getting tested at approved testing sites or using an FDA-authorized at home test," said Attorney General Brian E. Frosh.

Consumers who do not receive timely test results or have other concerns about a laboratory performing a COVID test should file a complaint with the Office of Healthcare Quality at https://app.smartsheet.com/b/form/483176a200fc44858f42772adb9283d1. Consumers with billing concerns should contact the Maryland Attorney Generals' Health Education and Advocacy Unit at https://www.marylandattorneygeneral.gov/Pages/CPD/HEAU/ComplaintChooser.aspx or by calling 410-528-1840 or 410-230-1712 (en español).

Anyone who was tested by someone going door-to-door or was deceived into giving personal information over the phone for free government tests could be at risk for identity theft. Anyone with questions or concerns about identity theft should visit the Maryland Attorney General's Identity Theft Unit webpage at https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx for important information. Consumers can also contact the Identity Theft Unit at 410-576-6491 or 410-230-1712 (en español).

Consumer Alert: Marylanders Impacted by the 2021 T-Mobile Data Breach Should Take Steps to Protect Personal Information

BALTIMORE, MD (March 3, 2022) – **Maryland Attorney General Brian E. Frosh** urges all Maryland residents impacted by the data breach announced by T-Mobile in August 2021 to take appropriate steps to protect their information from identity theft.

On August 17, T-Mobile reported a massive data breach compromising the sensitive personal information of millions of current, former, and prospective T-Mobile customers, including individuals who had applied for credit with T-Mobile. The breach impacted more than 53 million individuals, including over 1 million Maryland residents. Among other categories of impacted information, millions had their names, dates of birth, Social Security Numbers, and driver's license information compromised.

Recently, a large subset of the information compromised in the breach was for sale on the dark web—a hidden portion of the Internet where cyber criminals buy, sell, and track personal information. Many individuals have since received alerts through various identity theft protection services informing them that their information was found online in connection with the breach, confirming that impacted individuals are at heightened risk for identity theft.

Attorney General Frosh urges anyone who believes they were impacted by the T-Mobile breach to take the following steps to protect themselves:

- **Monitor your credit.** Credit monitoring services track your credit report and alert you whenever a change is made, such as a new account or a large purchase. Most services will notify you within 24 hours of any change to your credit report.
- **Consider placing a free credit freeze on your credit report.** Identity thieves will not be able to open a new credit account in your name while the freeze is in place. You can place a credit freeze by contacting each of the three major credit bureaus:
    - Equifax | https://www.equifax.com/personal/credit-report-services/credit-freeze/

+1 (888) 766-0008
    - Experian | https://www.experian.com/freeze/center.html
      +1 (888) 397-3742
    - TransUnion | https://www.transunion.com/credit-freeze
      +1 (800) 680-7289
- **Place a fraud alert on your credit report.** A fraud alert tells lenders and creditors to take extra steps to verify your identity before issuing credit. You can place a fraud alert by contacting any one of the three major credit bureaus.
- **Additional Resources.** If you believe you are a victim of identity theft, contact the Attorney General's Identity Theft Unit for assistance on how to report and recover from it: idtheft@oag.state.md.us or 410-576-6491.

Consumer Advisory: Protecting Yourself Against Mobile Payment App Scams

Mobile payment apps can easily send fast money to other people – splitting a dinner check with your friends, sending emergency money to your children, paying for merchandise or a service, or even buying stocks and cryptocurrency. They can eliminate the need for you to carry cash, and are often easier to use than swiping a bank card. But the ease and convenience of mobile payment apps is also the reason they are susceptible to thieves and scammers. These apps don't generally offer the same protection as other payment methods. So, if you do use them, inform yourself about the risks and exercise good practices for protecting your money. Some of the most popular mobile payment apps include Cash App, Venmo, and Zelle.

If you are defrauded into sending money using a mobile payment app, your bank may not refund the lost funds. This is because, in many cases, the victim has "authorized" the transfer, even if they were tricked into doing so. Laws concerning the definition of "authorized" when it comes to electronic transfer of funds are murky (for information on federal regulations regarding electronic fund transfers, visit the Consumer Financial Protection Bureau). The best approach to using these apps is to treat any transferred funds as you would cash.

Mobile payment apps are a favorite tool for scammers, especially romance swindlers and cryptocurrency fraudsters. But scammers can impersonate any number of contacts you may have and trust, including banks and creditors, friends and family, employers, "tech support," government agencies, or even payment app "representatives." Don't send any money unless you know the person to whom you are sending the money, and have confirmed the authenticity of that request.

Because mobile payment apps are often linked directly to your bank account, a thief could drain your funds in a matter of seconds, and you are unlikely to get that money back.

If you do choose to use mobile payment apps – and let's face it, they are convenient – you can take steps to avoid scammers:

- Don't send money to ANYONE you don't recognize, for any reason.

- If someone you do know requests money from you, call that person to confirm that they indeed made that request to you, even if you've sent them money through the app before.
- Never give anyone access to your account, even if they tell you that they need access to fix a problem or help you recoup lost money.
- Don't feel obligated to share your contact lists with the app. If the idea of the app having access to your contacts makes you uncomfortable, deny that access.
- Regularly review statements for any bank accounts linked to the app. Contact the bank and the app customer service if you see any transactions that you didn't authorize. IMPORTANT NOTE: Many mobile payment app customer services are notoriously difficult to connect with. Many apps do not have telephone numbers, but require you to contact them through email, text, or chat platforms. This means that simply performing an internet search for an app's customer service contact information can lead you right into a scammer's trap. Always use the app or the app's official website, if there is one, to contact its customer service.
- Set up two-factor authentication on your app.
- Secure your mobile devices at all times. If you provide access to your mobile device and someone, without your permission, transfers money to themselves using your mobile payment app, you could be responsible for the withdrawal.

If you purchase merchandise or a service using a mobile payment app, and are dissatisfied with the product, contact the business to see if you can resolve your complaint. If you aren't able to resolve your complaint to your satisfaction, the Attorney General's Consumer Protection Division may be able to mediate on your behalf. You can file a complaint through the Attorney General's website, www.MarylandAttorneyGeneral.gov, or email consumer@oag.state.md.us or call 410-528-8662 (en español 410-230-1712) for assistance.

If you are scammed or tricked into transferring money using a mobile payment app, your options are, unfortunately, limited for recouping that money. But you should report the fraud to your financial institution as soon as possible. You also should report the scam to help investigators track these crimes. You can report the scam to the app's customer service, the Consumer Protection Division, and the Federal Trade Commission.

Additional Resources

- Office of the Commissioner of Financial Regulation, Maryland Department of Labor, Consumer Resources
- Consumer Financial Protection Bureau
- National Consumer Law Center, Fintech, Electronic Payments and Remittances

Consumer Alert: Phishing Scam Targets Unemployment Insurance Claimants in Text Messages

The Office of the Attorney General has been made aware of a scheme in which fraudsters are impersonating the Maryland Department of Labor, Division of Unemployment Insurance in text messages.

To protect yourself from fraud, access your BEACON claimant portal by typing the following web address into your browser (https://beacon.labor.maryland.gov/beacon/claimant-page.html), or use the MD Unemployment for Claimants mobile app. If you receive text message, or an email, that appears to be from the Maryland Department of Labor, **DO NOT click on any links** in the message. Fraudulent websites that are impersonating the Department of Labor can look very similar to the real website. In the reported message, the fraudulent link began "mdgovapp.us."

If you believe that your information has been used to fraudulently file an unemployment insurance claim in Maryland, you must contact the Maryland Department of Labor. Complete the Request for Investigation of Unemployment Insurance Fraud form and email it to ui.fraud@maryland.gov.

To read about other ways to protect yourself from scams, fraud, and identity theft, visit our Consumer Protection Division publications page.

https://www.marylandattorneygeneral.gov/press/2022/032822CA.pdf

CONSUMER ADVISORY: What Is Home Title Lock Insurance, and Do You Really Need It?

You may have heard a radio ad lately with a dire warning that your home can be stolen right out from under your nose, and the solution they are peddling is to buy "title lock insurance." But what exactly is this service? Is it something you really need to keep your home safe from property thieves? Are there other safeguards already in place to protect the deed to your home? We're going to answer these questions so you can make an informed decision about whether you need to purchase this service for yourself.

What is title lock insurance? First, title "lock" insurance is NOT title insurance. These are two very different things. According to the Maryland Insurance Administration: "Title insurance protects real estate purchasers and/or lenders from losses that arise after a real estate settlement, but result from unknown liens, encumbrances or other defects upon the title that existed prior to settlement." Title LOCK insurance – which is not actually insurance of any kind – claims to protect you against title fraud, not against a legitimate challenge to the title. Title "lock" is a service that monitors the deed to your home to see if it has been transferred out of your name. The service will notify you if this happens – after it has already happened. These services do not actually "lock" your title to prevent fraudulent deed transfers.

Do you need this service to protect your home from property thieves? The answer is no. Title fraud is very rare, and hardly ever successful. If someone ever tries to transfer your deed without your permission or knowledge, like these title lock companies suggest could happen, the transfer is fraudulent and void from the outset. You can periodically perform the same check on your title, for free, as these "monitoring" services do for a fee.

Monitoring your identity is the best way to stop fraud in its tracks and prevent further damage from occurring. Pay attention to missing bills (for example, if you always receive a paper utility bill, and all of a sudden stop receiving one), check your credit with the three major credit reporting companies (Experian, TransUnion, and Equifax), and, as mentioned above, periodically check your title with your state land records office.

The bottom line is: You don't need to purchase title lock insurance. It neither locks nor insures your home title against fraud. You should consider freezing your credit reports, which will make it difficult for a fraudster to open new accounts in your name. You also should keep your personal and financial information secure, check your credit, don't give out your Social Security Number, and destroy any documents with personal information that you no longer need. More information about protecting your identity is available on the Attorney General's website.

https://www.marylandattorneygeneral.gov/press/2022/062722CA.pdf

Consumer Advisory: Some Medical Debt No Longer Reported on Certain Credit Reports

Starting today, July 1, 2022, three major credit reporting agencies – Experian, Equifax, and TransUnion – will no longer report paid medical debt on reports about your credit-worthiness that are issued by these companies. This means, for example, that if you apply for a credit card or a lease on an apartment, old paid medical debt will not show up on the report issued to the credit card company or potential landlord.

In addition, the time for consumers to resolve outstanding unpaid medical debts that have been sent to collections has been extended by the credit reporting agencies from six months to one year before the debt is included on a credit report.

Next year, medical debt under $500 will no longer be included on these reports, whether or not it has been paid.

Our office's Health Education and Advocacy Unit (HEAU) reminds consumers to carefully review medical bills and, if insured, to compare them with the explanation of benefits provided by their health insurance providers. If consumers believe there is a medical billing error that they can't resolve with their healthcare provider, our HEAU can help mediate the dispute. The HEAU can be reached by telephone at 410-528-1840 (en español 410-230-1712) or heau@oag.state.md.us. More information about the HEAU can be found at www.marylandcares.org.

It's always a good idea to regularly review your credit reports to make sure the information is accurate and complete. To check your credit report for free, visit www.annualcreditreport.com. Maryland law provides you with the right to obtain a second free credit report each year from each of the major credit reporting agencies in addition to the free annual report under federal law.

https://www.marylandattorneygeneral.gov/press/2022/070122CA.pdf

Consumer Advisory: "Buy Now, Pay Later" Plans Can Lead to Unintentional Debt, Other Problems

Installment plans for retail shopping are becoming increasingly popular, especially those that promise no interest – if paid on time. These programs allow you to buy a product and pay only a fraction of the cost at a time – weekly or monthly, for example – with little or no interest accruing. Unlike layaway, you can receive your item right away, before it's paid off. But be careful: These payment plans 1) can make items appear cheaper than they really are, blowing your budget out of the water, 2) could cause you to accumulate debt, especially if you don't pay on time or miss a payment, and 3) don't help you build credit the way credit cards and traditional consumer loans do.

Installment payment plans are basically short-term loans. If you do apply for this option, the creditor will check your credit to see if you qualify for the plan. If the plan is interest-free, which many are, it generally means that interest won't accrue if you pay each installment, *on time*. Otherwise, you could be charged back-interest and/or other fees, piling up debt you didn't anticipate.

These plans are convenient if you really need a product, such as an emergency appliance replacement, but don't have the cash or a credit card to make the purchase. But if you're buying multiple items on multiple payment plans, beware that you may end up paying more and damage your credit if you don't pay on time. In addition, returns and exchanges can be complicated, so make sure that you understand the return process before you make your purchase.

Only you can decide if these payment plans are right for you. If you do apply for one, be sure you can pay off the item in the time stipulated. Stick to your budget, and look at the entire price of the merchandise, not just the installment payment amount. Make sure you're aware of all fees, and how your credit could be harmed if you fail to make the payments on time.

If you have a problem with an installment payment plan creditor, contact the Consumer Protection Division at 410-528-8662 or email consumer@oag.state.md.us.

https://www.marylandattorneygeneral.gov/press/2022/070822CA.pdf

Consumer Alert: Attorney General Frosh Warns Consumers about Purchasing Flood-Damaged Cars

BALTIMORE, MD (October 12, 2022) – Maryland Attorney General Brian E. Frosh today warned consumers to be cautious of purchasing vehicles that may have been impacted by major flood damage. After hurricanes with large-scale floods like Ian, flood-damaged cars often end up at salvage auctions and bought by rebuilders. While these vehicles should be marked "salvage" or "total loss" on the title, dishonest sellers may "wash" the title, hide the damage, and offer these vehicles for sale.

"Consumers purchasing a used car after a hurricane should always be wary that the vehicle may be irreparably damaged and not the good deal it appears to be," said Attorney General Frosh.

Signs of a flooded vehicle may include:

- A musty odor in the interior, which might be covered with a strong air-freshener;
- Upholstery or carpeting which is loose, stained, doesn't match, is new, or is damp;
- Rust around doors, under the dashboard, on the pedals, or inside the hood and trunk latches;
- Mud or silt in the glove compartment or under the seats;
- Brittle wires under the dashboard; and/or
- Fog or moisture beads in the interior or exterior lights or instrument panel.

Attorney General Frosh advises consumers to follow these tips to protect themselves and avoid purchasing flood-damaged vehicles:

- Check the VIN history. The National Insurance Crime Bureau (NICB) has a free database that can tell you if a car has been marked as salvage, stolen, etc. Note, rental vehicles may not make it into this database. Consumers can check the vehicle history by visiting: www.nicb.org/theft_and_fraud_awareness/vincheck
- Check the title. If the VIN number clears the NICB, consumers should then check the National Motor Vehicle Title Information System, a program administered by the U.S.

Department of Justice, at: www.vehiclehistory.gov/nmvtis_vehiclehistory.html. There may be a fee to obtain reports through this service. The history reports provide current and previous state of title data, title issue date, latest odometer data, theft history data (if any), any brand assigned to a vehicle and date applied, and salvage history, including designations of a "total loss" (if any).

- Additional resources. If the VIN and title checks clear, consumers may use paid sources, such as CarFax or AutoCheck.
- Inspection: Consumers should thoroughly inspect their prospective vehicles, even if the vehicle clears all reports. Salvagers clean vehicles extensively. However, not all flood damage is visible.

Consumers who suspect they may have purchased a flood-damaged vehicle may file a complaint with the Office of Attorney General's Consumer Protection Division by visiting www.marylandattorneygeneral.gov.

https://www.marylandattorneygeneral.gov/press/2022/101222CA.pdf

Consumer Alert: Home Warranty Scam Letters Sent to Maryland Homeowners

The Consumer Protection Division of the Maryland Attorney General's Office is warning consumers about home warranty scam letters addressed to homeowners.

These letters urge Maryland homeowners to renew a home warranty by claiming the current home warranty "may be expiring or may have already expired." Even homeowners who have never purchased a home warranty are receiving this deceptive letter. The letters also imply an affiliation with the homeowner's actual mortgage company and the "county deed records" office. The scammers responsible for these letters are in no way affiliated with the homeowner's mortgage company or any official deeds office.

These letters generally ask for a response to the notice by a certain date, often include language such as "final notice," and threaten that failing to call may result in financial risk for the homeowner. In examples of such a letter sent to the Attorney General's office, also included are a document that resembles a check, with the words "renewal fee voucher," as well as an actual photo of the homeowner's home on the return envelope.

Solicitations that use threatening language or unnecessary urgency are almost always a scam. Although they include the name of the homeowner's mortgage company, scam letters like this rely on publicly available information to deceive the homeowner. To reiterate, the people sending these letters are not representing, nor have any affiliation with, mortgage companies. They use this information, as well as other seemingly "official" references, such as "record ID" numbers, to appear legitimate. If you have a home warranty, check with the company through which you already purchased your warranty for expiration and renewal information.

If you are interested in purchasing a home warranty with a legitimate company, conduct thorough research about potential businesses by reading reviews, checking with the Better Business Bureau, and contacting our office to see if any complaints have been filed against a particular business. As for these scam letters, we recommend that you report them to our office at consumer@oag.state.md.us, and then discard them. Do not call any numbers listed on the solicitation, or respond to them in any way.

https://www.marylandattorneygeneral.gov/press/2022/112922CA.pdf