BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

PRESS RELEASE

Attorney General Frosh Warns Marylanders About DNA Testing Scam Targeting Medicare and Medicaid Beneficiaries

BALTIMORE, MD (May 8, 2019) – Maryland Attorney General Brian E. Frosh is warning consumers to be suspicious of representatives of companies that purport to offer "free" DNA testing to check for cancer. The DNA testing scam is a new twist used by scammers to trick people into giving away their health insurance information for the purpose of committing identity theft and fraud.

Scammers are targeting Medicare beneficiaries with phone calls and by visiting health fairs, assisted living homes, and senior events. Claiming the DNA testing is covered by Medicare, they will use a cotton swab stick to a take a saliva sample from the inside of your mouth. They request your Medicare information and may also ask for your social security number. Do not be fooled; this is a scam. *Medicare only pays for certain genetic testing and cancer screenings that are medically necessary and ordered by a doctor*.

In other states, scammers have also targeted Medicaid beneficiaries by claiming to be affiliated with a local Medicaid insurer. In Louisville, Kentucky, scammers paid $20 to Medicaid recipients as an incentive for them to take a DNA test, and subsequently requested their Medicaid insurance information. It is illegal to pay anyone who is a recipient of government health insurance to induce them to receive a medical service.

Although the Maryland Office of Attorney General has received a small number of complaints, other states across the country have received numerous complaints about the DNA testing scam, which may be the work of an organized group or individuals acting alone.

The scam raises concerns about potential health care fraud and identity theft since scammers have the names of consumers and their health insurance information. This information could be sold to unscrupulous health care providers who may bill Medicare and Medicaid for medical services that were not provided to the consumer. It could also be used by an imposter to obtain free medical care using your identity and health insurance information.

It is unclear if the genetic samples or test results are being misused or sold for other illicit purposes. Authorities in other states have found evidence of cheek swabs being discarded rather than sent away for actual genetic testing at health fairs.

“These scammers prey on vulnerable individuals, exploiting them for profit and potentially to steal their identities,” said Attorney General Frosh. “I encourage anyone who has been a victim of this ‘DNA’ scam or seen it carried out within their community to immediately report it to our Health Education and Advocacy Unit by calling 410-528-1840 or toll-free at 1-877-261-8807.”

Here are some additional tips on how to protect yourself against the DNA testing scam:

- Be suspicious of anyone offering free DNA tests and cancer screenings. Only a doctor can determine if such testing is medically necessary for you. Be suspicious of anyone offering to pay you to take a DNA test; it is against the law for Medicare or Medicaid beneficiaries to receive payment in exchange for undergoing medical tests.
- Never share your Medicare or Medicaid insurance number (or Social Security Number) with anyone who offers free medical products or medical services.
- Monitor your credit reports for unauthorized activity and your Medicare statements for suspicious charges, especially if you have shared your personal medical information with anyone offering a free DNA test.
- Call 1-800-Medicare (1-800-633-4227) or 1-800-HHS-TIPS if you think you have been the victim of Medicare fraud. Contact the Maryland Department of Health’s Program Integrity Division at 1-866-770-7175 if you believe you have been the victim of Medicaid fraud.

BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

PRESS RELEASE

Consumer Alert: Attorney General's Office Receives Reports of Imposter Law Enforcement Scam

BALTIMORE, MD (June 3, 2019) – Maryland Attorney General Brian E. Frosh is warning consumers of a scam in which thieves posing as law enforcement swindle money from Marylanders by threatening arrest for missing jury duty or failure to appear as a witness.

Anyone can fall victim to this sophisticated scam. Reports indicate that it is affecting Marylanders in several counties. Here is what consumers report.

The scammer calls a potential victim, claiming falsely to be calling from a local police department or sheriff's office to tell them that they have missed a court date. The scammer may leave a message for a call back, and the caller ID often indicates a local area code. If the victim calls the number back, a recording suggests that they reached a legitimate law enforcement office. Once the caller is connected to a live person, that person tells the victim they missed jury duty, that a certified notice was signed by someone at their home, and that a bench warrant for their arrest has been issued for failure to attend jury duty and contempt of court.

In some reported cases, the scammer tells the victim that they must meet in person to resolve the issue. The scammer may provide the victim with an address belonging to an actual law enforcement location to appear legitimate. But once the victim arrives at that location, the scammer will then ask for payment (generally by gift card, prepaid cash card, or wire transfer) to immediately resolve the issue.

In other cases, the scammer tells the victim that there is a fine due for missing the court appearance, and that the victim *cannot* go to the local law enforcement department or they will be arrested. The scammer tells the victim that they can only pay the fine by wiring funds—no cash or checks are accepted. They may also tell the victim that if they pay the fine within a designated time that they only need to pay a portion of the fine.

Once the victim agrees to pay the fine, the scammer provides instruction on how to pay, and then will likely tell the victim that they must stay on the phone until the payment is complete. In a complaint received by the Consumer Protection Division, the scammer instructed the victim to use a MoneyPak card to pay the fine.

In addition to the above, the scammer may tell the victim that there is a "gag order" on their case so they cannot talk about it. They may also ask the victim to scan and email a copy of their driver's license.

Under no circumstances should you pay any money, whether through MoneyPak or any other quick money transfer, to any person or group that claims to be a law enforcement officer even if they threaten you with arrest or fine. Nor should you email or reveal by telephone any personal information to anyone unless it is an exchange that you initiated.

If you do receive a call that tries to extort you in this way, follow these steps:

1. Hang up immediately.
2. Do NOT call the number shown on the caller ID.
3. Do NOT send your driver's license information to anyone who calls claiming to be a law enforcement officer.
4. Report the suspicious call to the Office of the Attorney General or the Federal Trade Commission.

If you have received a call like this and paid the caller any amount of money, or revealed any personal information via email or by phone, follow these steps:

1. Contact the company that facilitated the funds transfer to see if you can stop the payment.
2. Contact the Attorney General's Identity Theft Unit to learn how to protect yourself if the scammers try to use your personal information.
3. Contact your local law enforcement department to report the theft.
4. Report the incident to the Office of the Attorney General or the Federal Trade Commission.

"Only one person has to fall for this scam for the thieves to potentially make hundreds of dollars," said Attorney General Frosh. "These scammers are very good at persuading anyone that they are in trouble with the law. But remember that legitimate law enforcement officers will NEVER ask you to pay a fine by wire transfer or any other rapid money transfer."

The Maryland Courts have also issued an alert about this scam. Call our Consumer Protection Hotline at 410-528-8662 to speak with someone if you have questions about this or any other scam.

BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

PRESS RELEASE

Maryland Attorney General Joins Partnership to Combat Elder Financial Abuse
PROTECT Week 2019 Events to Take Place Statewide, World Elder Abuse Awareness Day Is June 15

BALTIMORE, MD (June 10, 2019) – To assist Marylanders in identifying and combatting fraud, especially against seniors and other vulnerable adults, the Office of the Attorney General, is participating in a statewide public awareness campaign during PROTECT Week (Protecting Older Americans from Financial Exploitation), June 10–15, 2019. Other partners of this campaign include AARP Maryland, Consumer Credit Counseling Service of Maryland, the Maryland Department of Aging, the Commissioner of Financial Regulation, the Office of the Comptroller, and other consumer protection groups.

PROTECT Week events include anti-fraud workshops and opportunities to shred sensitive documents to keep them out of the hands of identity thieves. Maryland Attorney General Brian E. Frosh will be attending a press conference at Atrium Village in Owings Mills on Tuesday, June 11 at 10:30 AM, and additional events in Howard, Baltimore, Prince George's, and Garrett Counties are scheduled throughout the week. The full schedule of events is available at www.protectweek.org. All PROTECT Week events are free and open to the public, but registration is required.

On June 14, 10:00 to 11:00 AM, AARP Maryland will host a telephone town hall with Attorney General Frosh, Comptroller Peter Franchot, Commissioner of Financial Regulation Antonio Salazar, Office of Adult Services Director Dorinda Adams, and CCCSMD President Helene Raynaud. Callers will learn how to identify, prevent, and report fraud and have the opportunity to ask the panel of experts questions about fraud prevention.

In Maryland more than 54,000 cases of fraud were reported in 2018, according to the Federal Trade Commission, with losses totaling more than $18 million. An increasingly common scheme is the "grandparent" scam, in which callers pretend the victim's relative is in jail and needs bail money wired. Other popular cons include "lottery scams," in which victims are persuaded that they have won a contest and have to send money upfront to pay the taxes before receiving their winnings, and "tech support" scams, in which thieves seek to gain access to the victim's personal computer through phone calls, emails, or "pop-up" ads on the computer.

"One of my office's highest priorities is protecting seniors and vulnerable adults from financial abuse by way of deception, intimidation, or undue influence," said Attorney General Frosh. "Sadly, these abuses can be perpetrated by close 'friends and family' as well as complete strangers."

Reporting financial exploitation of elders can help put a stop to this kind of abuse. If you have questions about financial exploitation, think you or a loved one may have been a victim, or need guidance navigating a number of other consumer issues, contact the Attorney General's Consumer Protection Division at 410-528-8662.

BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

CONSUMER ALERT

Consumer Alert: Attorney General Frosh Warns Marylanders of Massive Medical Data Breach

American Medical Collection Agency Experienced Cyberattack; Patient Personal Data May Be at Risk

BALTIMORE, MD (June 12, 2019) – Maryland Attorney General Brian E. Frosh is warning Marylanders that their medical and other private information may have been compromised by a cyberattack against American Medical Collection Agency (AMCA), a third party collection agency for laboratories, hospitals, physician groups, medical providers, and others.

Presently, the known list of impacted entities affects over 20 million patients. The list is likely to expand and includes the following entities:

- Quest Diagnostics: 11.9 million patients
- LabCorp: 7.7 million patients
- BioReference Laboratories: 422,600 patients
- Carecentrix: 500,000 patients
- Sunrise Laboratories: unknown number of patients

The compromised information varies for each entity, but includes some or all of the following information: patient name, date of birth, address, phone number, date of service, provider, balance information, payment card information, bank account information, social security number, and the lab test performed.

AMCA's payment system was compromised on August 1, 2018, and remained vulnerable through March 30, 2019. AMCA has started sending out written notices to consumers whose credit card number, social security number, or lab test order information may have been accessed.

Recent reports of massive data breaches highlight the need for Marylanders to be vigilant about their personal information and aware of how it may be compromised and misused. The Maryland Personal Information Protection Act (PIPA) requires any business that keeps electronic records containing the personal identifying information of Maryland residents to notify those residents if their information is compromised.

Consumers should always carefully review their financial and medical account regularly for suspicious activity and immediately report all suspicious or fraudulent charges to their financial

institutions or health insurance providers. Consumers impacted by the AMCA data breach should be especially vigilant.

"Massive data breaches like the one experienced by the AMCA are extremely alarming, especially considering the likelihood that personal, financial, and medical information may now be in the hands of thieves and scammers," said Attorney General Frosh. "I strongly urge consumers to take steps to ensure that their information and personal identity is protected."

Consumers who believe they may have been affected by this breach should immediately take the following steps to protect their information:

- Obtain a free credit report at www.annualcreditreport.com or by calling 877-322-8228.
- Put a fraud alert on your credit file.
- Consider a security freeze on your credit file (for more information about freezes, visit http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/freezing.aspx).
- Take advantage of any free services being offered as a result of the breach.
- Use two-factor authentication on your online accounts whenever available.

The Office of the Attorney General has an Identity Theft Unit that offers guidance and assistance. Information about protecting yourself or your children against identity theft, and what to do if it occurs, can be found at www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx.

If consumers feel they have been harmed and want to file a complaint, they may call the Attorney General's Identity Theft Unit at 410-576-6491.

BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

CONSUMER ALERT

Scammers Are Sending Fake Checks to Swindle Consumers Out of Thousands of Dollars

BALTIMORE, MD (July 23, 2019) – Scammers are sending fake checks that appear to be from Maryland-based Chesapeake Employers Insurance Company (CEIC) and the Injured Worker's Insurance Fund (IWIF) to unsuspecting victims all over the country. Please note that this scam does NOT affect CEIC or IWIF claimants or other persons receiving legitimate checks from these companies.

This is how the scam works: a person reaches out to a victim through Facebook and promises to send them a check in exchange for performing some type of work. The victim receives a falsified check that appears to be from CEIC or IWIF, and is told that they can keep part of the money once they accept the check and do the work. Once the victim deposits the check, the funds appear in their account as "pending." However, these checks are eventually declined by the bank, and any money the victim sent back to the scammer in the meantime is gone for good and the victim is never paid for any "work" they did on behalf of the scammer. In this particular scam, victims have lost thousands of dollars, some as high as tens of thousands of dollars.

This particular kind of scam is performed often and is not unique to CEIC and IWIF. The Consumer Protection Division is warning anyone who receives a check from an individual or business that they don't know for work performed, or with instructions to keep a portion of the money and send the rest elsewhere, to be very suspicious: this is most likely a scam. Other scammers may reach out with a "job offer," promising to send a check to get you started. Clues this is scam include correspondence and/or checks that are sent from overseas or from an address different than the supposed location of the "employer." If an individual reaches out to you through social media with these kinds of "offer," ignore and block them.

If you do receive a check that you're not expecting or that appears suspicious, be extra cautious. Contact the company whose name is on the check and ask them if they sent you a check and why. Only after you have verified with this company that the check is legitimate should you deposit it into your bank account. If you are asked to deposit a check and to return a portion of the funds to the sender, it is almost certainly a scam and you will lose the money that you send.

If you've been the victim of a scam, please contact the Consumer Protections Division's hotline at 410-528-8662 or toll-free 1-888-743-0023.

BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

CONSUMER ALERT

Consumer Alert: Attorney General Warns Marylanders Regarding the Capital One Data Breach

BALTIMORE, MD (July 30, 2019) – Maryland Attorney General Brian E. Frosh is warning Marylanders that their personal and credit data may have been compromised in the July 19, 2019, data breach experienced by Capital One, the national bank and credit card issuer. Earlier this week, Capital One announced that a hacker had accessed about 100 million credit card application files. The hacker, based in Seattle, has already been arrested and, according to a complaint filed by the FBI, no evidence has yet been revealed that the stolen information was sold or disseminated by the hacker to any third party.

The compromised information reportedly included consumers' Social Security numbers, the majority of which were tokenized or encrypted. About 144,000 of the compromised Social Security numbers, which were used as employer identification numbers when applying for small business credit cards, were accessed by the hackers. Other information that was reportedly compromised in the breach included applicant's names, addresses, dates of birth, and information regarding their credit history (e.g., credit scores, credit limits, balances, payment history, and contact information). Capital One has stated that no credit card numbers or log-in credentials were compromised.

Capital One is providing information regarding the breach at the following link on its website: www.capitalone.com/facts2019/. It has announced that it will be notifying affected consumers and providing them with free credit monitoring.

Consumers who believe they may have been affected by a data breach should consider taking the following steps to protect their information:

- Obtain a free credit report at www.annualcreditreport.com or by calling 877-322-8228.
- Put a fraud alert on your credit file (you only need to contact one of the three major credit reporting agencies (Equifax, Experian, or Transunion) to place a fraud alert).
- Place a security freeze on your credit file (for more information about freezes, visit http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/freezing.aspx).
- Take advantage of any free services being offered as a result of the breach.
- Use two-factor authentication on your online accounts whenever available.

The Office of the Attorney General has an Identity Theft Unit that offers guidance and assistance. Information about protecting yourself or your children against identity theft, and what to do if it occurs, can be found at www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx. If consumers feel they have been harmed and want to file a complaint, they may call the Attorney General's Identity Theft Unit at 410-576-6491.

Brian E. Frosh
Attorney General

Media Contacts:
Press@oag.state.md.us
410-576-7009

Consumer Alert

Consumer Alert: Attorney General Warns Marylanders About "Community Development Block Grant" Scam

BALTIMORE, MD (November 13, 2019) – Maryland Attorney General Brian E. Frosh is warning Marylanders that scammers are contacting individuals claiming they are entitled to, or have been awarded a "Community Development Block Grant," "Community Services Block Grant," or "CSBG for seniors." This is a scam to obtain personal information and/or money in the form of upfront "fees" (in one reported case, the scammer asked for $1,000 in gift cards). There have been reports of these scammers reaching out through email and text messaging, but they could also reach out to potential victims by phone.

Marylanders should disregard and delete immediately any messages that claim they have won or are entitled to a community block grant or similar-sounding name. Hang up on any person who calls claiming that you have been awarded one of these grants. While the Community Services Block Grant and Community Development Block Grants do exist, both are administered by the Maryland Department of Housing and Community Development. These Programs are administered as part of a U.S. Housing and Urban Development (HUD) program intended to distribute federal funds directly to state governments, local jurisdictions, and non-profits for housing and other social services programs. These grants are NOT awarded to private citizens.

If you have not directly applied for a grant or aid, the chances are extremely high that someone offering to "award" you one is a scam artist. Do not send money or gift cards to anyone requesting upfront fees or taxes on a grant, award, or anything else they claim you have "won." Requesting money or prepaid debit/credit or gift cards is a red flag that you are being targeted by a scammer.

You can report these messages to the Consumer Protection Division of the Office of the Attorney General (www.marylandattorneygeneral.gov) or the Federal Trade Commission (www.ftccomplaintassistant.gov).

BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

CONSUMER ALERT

Consumer Alert: Attorney General Warns Marylanders About Scam "Winning Lottery" Letter

BALTIMORE, MD (November 18, 2019) – Maryland Attorney General Brian E. Frosh's Consumer Protection Division is warning consumers of a "lottery" mail scam targeting Marylanders. The scam letter claims the recipient has won the "Mega Millions International Lottery 2019 Draw" and includes a counterfeit reproduction of the Maryland Mega Millions logo. The sender of the letter has **no affiliation** with the Mega Millions Consortium, which is the group of United States Lotteries organized to jointly create and operate the multi-state lottery game known as Mega Millions.

The letter reported to the Attorney General's office is purported to be from the "International Promotion Price Award Dept.," includes several logos including that of Mega Millions and the United Nations, asks the recipient to call a foreign number or send an email to claim their lottery "winnings," establishes a deadline for the recipient to contact the lottery company, claims that the lottery company will need to be paid a percentage of the "winnings," and that the lottery company can pay the recipient by wire transfer to their bank account.

Here are some tips to avoid being scammed by "lottery" letters, email, or texts.:

- Do not under any circumstances send money by wire, funds transfer, gift cards, or cashier's check to anyone claiming you need to pay a fee to receive an award or lottery winnings, particularly one you didn't specifically enter.
- Do not give your bank routing or account information to anyone so they can "deposit your winnings." The money in your bank account could be wiped out in seconds.
- Be wary of urgent requests to "act now"; scammers will often create a false sense of urgency to get you to respond without thinking carefully.
- Do not click on any links or call any numbers in a suspicious email or text; even if the links look official, they could redirect you to a harmful website or download viruses onto your phone or computer.
- If it looks too good to be true, like winning millions of dollars from a foreign lottery, it probably is.

If you receive a letter like the one described above, or any letter claiming you have won an "international" lottery, **throw it away**! Unless you specifically entered a Maryland Lottery promotion, you will never be contacted by Lottery officials informing you that you have won a prize. Under Maryland law, it is unlawful for a person, another state, or foreign government to

sell a lottery ticket in the State of Maryland. You may visit https://www.mdlottery.com/about-us/fraud-prevention/ for more information about fraud prevention.

If you receive any materials at your home address regarding another state's lottery or a foreign government's lottery, please forward that information directly to the U.S. Postal Inspection Service Mail Fraud division through https://www.uspis.gov/report/, or you may call 1-800-372-8347. You can also report receiving these letters to the Attorney General's Consumer Protection Division (www.marylandattorneygeneral.gov) and Federal Trade Commission (https://www.ftccomplaintassistant.gov/).

BRIAN E. FROSH
ATTORNEY GENERAL

MEDIA CONTACTS:
PRESS@OAG.STATE.MD.US
410-576-7009

PRESS RELEASE

Attorney General Brian Frosh and BGE Join Together for Annual Utility Scam Awareness Day

BALTIMORE, MD (November 20, 2019) – Maryland Attorney General Brian E. Frosh is joining with BGE to promote awareness of utility service scams and provide helpful advice for avoiding them. In the last three years, 61 utility scam complaints have been received by the Attorney General's Consumer Protection Division. Some victims have reported losing as much as $4,000 dollars to a utility service scam.

For the fourth year in a row, BGE is joining more than 140 energy companies across the United States and Canada in the effort to protect customers from scams targeting customers of electric, natural gas, water, and other utilities. Collaborating energy companies have joined together and designated November 20 as "Utilities United Against Scams Day." This effort is supported by a week-long campaign, including social media and online content, focused on exposing the tricks scammers use to steal money from customers, and how customers can protect themselves. The effort, which includes industry organizations such as Edison Electric Institute and American Gas Association, encourages companies to share these messages to help guard against scam and imposter activity.

"Utility scammers use fear and intimidation to get you to believe your electricity, water, or other utility shut off is imminent," said Attorney General Frosh. "Legitimate utilities would never give only one hour's notice. These scammers don't just go after individuals; business owners should also be suspicious if they receive a call or visit from someone threatening to shut off a utility. Always contact the utility directly using the telephone number on your bill if you suspect there is problem."

"Utilities United Against Scams Day is very important for BGE," said Rodney Oddoye, vice president and chief customer officer for BGE. "Unfortunately, scammers are constantly changing their tactics, which is why it is so important that our customers have tools and information to help them avoid becoming victims."

It is not uncommon for scammers to call, text, or email utility customers asking for immediate payment to avoid service disconnection. As a reminder, utilities will never send a single notification to a customer within one hour of a service interruption, and they never will ask their customers to make payments with a pre-paid debit card, gift card, or any form of cryptocurrency.

Scammers have even duplicated the upfront Interactive Voice Response system of some companies, so when customers call the number provided by the scammer, it sounds like a

legitimate business. Some scammers also use caller ID "spoofing" to replicate a utility's phone number.

Red flags for scam activity

- The scammer often becomes angry and tells a customer his or her account is past due and service will be shut off if a large payment isn't made—usually within less than an hour.
- The scammer instructs the customer to purchase a prepaid debit or credit card—widely available at most retail stores—then call him or her back to make a payment.
- The scammer asks the customer for the prepaid card's receipt number and PIN number, which grants instant access to the funds loaded to the card.

How to protect yourself

- Utility representatives will never ask or require a customer with a past due balance to purchase a prepaid debit card to avoid disconnection.
- Customers can make payments online, by phone, automatic bank withdrawal, mail, or in person.
- Customers with a past due balance will receive multiple shut off notifications—never a single notification one hour before disconnection.
- If a customer ever questions the legitimacy of the call, hang up and call BGE at 800-685-0123 or your utility service provider if you maintain service through another utility.

Don't Get Scammed. Customers can avoid being scammed by taking a few precautions:

- **Never provide your social security number or personal information** to anyone initiating contact with you claiming to be a utility representative or requesting you to send money to another person or entity other than your local utility providers.
- **Always ask to see a company photo ID** before allowing any utility worker into your home or business.
- **Never make a payment for services to anyone coming to your door.**

Any customer who believes he or she has been a target of a scam is urged to contact their local police and call BGE immediately at 800-685-0123 or your utility service provider to report the situation. You can also contact the Attorney General's Consumer Protection Division at 410-528-8662 or 888-743-0023 (toll free) to report the scam attempt or if you believe you have been a victim of a scam.