

PRESS RELEASE

Attorney General Frosh Warns Marylanders About Coronavirus Disease 2019 Scams

BALTIMORE, MD (March 6, 2020) – Maryland Attorney General Brian E. Frosh is warning Maryland residents to be on guard against scams involving the Coronavirus Disease 2019 ("COVID-19"). Scammers are setting up websites to sell bogus health products that claim to prevent or cure COVID-19, and using fake emails, texts, and social media posts about COVID-19 as a ruse to steal money and personal information.

"Scammers are taking advantage of people's fear of getting sick from COVID-19. Consumers can avoid being cheated by understanding how these thieves are trying to steal their personal information and money," said Attorney General Frosh.

Swindlers are posing as authorities, like the Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO). They send emails claiming to offer updated information about how people can protect themselves from COVID-19. Unsolicited emails from the CDC, WHO, or other "experts" saying they have information about the virus are likely phishing attempts to get money or personal information, or may be attempting to download viruses or malware onto the recipient's computer. The Attorney General's office advises Marylanders not to click on suspicious links online or in emails for information, but to seek information about COVID-19 from reliable sources such as government health agencies. For the latest, most accurate information about COVID-19, Marylanders can go directly to the CDC (www.cdc.gov), WHO (www.who.it), or the Maryland Department of Health (www.health.maryland.gov).

There are no approved vaccines, drugs, or treatment products specifically for COVID-19 available for purchase online or in stores. Pitches for any health product claiming to prevent or cure coronavirus are almost certainly fraudulent. The Food and Drug Administration (FDA) warns that fraudulent products not only fail to work, but they could also cause serious injury. Scammers may be promoting their fraudulent health products through newspapers, magazines, TV infomercials, email, social media sites like Facebook and Twitter, and online through websites and popup ads. Complaints against these fraudulent health claims can be filed with the Federal Trade Commission at <u>www.ftccomplaintassistant.gov</u> or the FDA (<u>www.fda.gov</u>).

Someone asking for donations - especially in cash, prepaid credit cards, gift cards, or bitcoin - to help victims of COVID-19, or for "research" into finding a vaccine or cure, is very likely a scammer. Sites like <u>www.charitynavigator.org</u> can be used to determine the legitimacy of a

charity. Donors can also contact the Maryland Secretary of State's Office at 800-825-4510 to verify that a charity is registered in Maryland as required by law.

The <u>U.S. Securities and Exchange Commission</u> (SEC) is warning people about online promotions, including on social media, claiming that the products or services of publicly-traded companies can prevent, detect, or cure coronavirus (and that investment in these stocks will increase in value). Investors may lose significant amounts of money if they invest in companies making fraudulent claims. Alternatively, these could be "pump-and-dump" schemes in which promoters hype up a stock, get many people to invest, and then sell off their own shares quickly for a profit—before the end of the hype makes the stocks worthless.

COVID-19 scams can be reported to our Consumer Protection Division by calling 410-528-8662, or by filing a report with WHO (<u>https://www.who.int/about/report_scam/en/</u>) or the FTC (<u>ftc.gov/complaint</u>).



CONSUMER ALERT

Consumer Alert: Per Governor's Order, Maryland Registered Vehicles Cannot Be Towed for Expired Registrations

In an effort to control and prevent the spread of the COVID-19 virus, Governor Hogan declared a State of Emergency in Maryland on March 5, 2020. This declaration affected the operations of many state agencies, including the Motor Vehicle Administration. On March 12, 2020, Governor Hogan ordered that expired vehicle registrations, and those that would otherwise expire during the State of Emergency, will remain valid until at least 30 days after the emergency has been ended.

This means that if a vehicle displays a registration that has expired, it may NOT be towed solely due to the expired registration.

If your vehicle is towed, or you are being threatened with a tow, solely due to an expired registration, please contact your county's towing board, or you can file a complaint with our Consumer Protection Division. Online complaints can be filed through www.marylandattorneygeneral.gov by clicking on the red "File a Consumer Complaint" button on the top left of the page.



CONSUMER ALERT

Beware of Coronavirus Aid, Relief, and Economic Security Act (CARES Act) Scams and Fraud

On March 27, 2020, the federal government passed the CARES Act, which aims to provide financial relief to individuals and businesses affected by the COVID-19 coronavirus pandemic here in the United States. Key provisions of the Act include direct payments to some individuals, based on income (a "stimulus check"); extended unemployment benefits; small business relief; no-cost testing for COVID-19; and more.

However, along with the Act comes a higher likelihood of scams and fraud schemes taking advantage of people unfamiliar with how these benefits work. Please take note of the information below to protect yourself against scams.

- Neither the State of Maryland nor the federal government will contact you by text, email, or call with instructions about receiving a stimulus check. Anything like that is likely just a ruse to steal your personal information or money. Any communication claiming to be able to get your stimulus check early is also a scam.
- Anyone who calls claiming to be from the government and asks for your Social Security number or any financial information (bank account number or credit card number, for example) is trying to scam you.
- You will NOT need to pay any money to the government, or anyone, before receiving a stimulus check.
- You do NOT need to complete the U.S. 2020 Census in order to receive a stimulus check.
- If you have questions about stimulus payments to individuals, communicate directly only with the IRS. More information is available at <u>www.irs.gov/coronavirus</u>.
- COVID-19 virus testing is always free, but it MUST be carried out by a qualified health care entity, such as your doctor or a hospital. Anyone claiming that they can sell you an at-home test is a fraudster.
- The federal Small Business Administration does NOT directly administer loans to small businesses. It backs other lenders (such as banks) to provide these loans to businesses. Any unsolicited contact from someone claiming to be able to get your business an SBA loan is a scammer.

"Scammers are hard at work trying to come up with ways to steal your personal information or money. Don't fall for it," said Attorney General Frosh. "If you need help determining whether something is a scam, our Consumer Protection Division can assist you. Call us at 410-528-8662 or email <u>consumer@oag.state.md.us</u>."



PRESS RELEASE

Attorney General Frosh Warns Consumers to Beware of COVID-19-Related Investment Schemes

BALTIMORE, MD (April 21, 2020) - Amid the ongoing COVID-19 pandemic, Maryland Attorney General Brian E. Frosh is alerting investors to be on guard against an anticipated surge of fraudulent investment schemes.

"In these extraordinary times the health and welfare of all must be our foremost concern, and that includes our financial health" said Attorney General Frosh. "Scammers will begin perpetrating schemes that require little or no advance planning and minimal sophistication. Most will simply be old scams dressed in contemporary clothing."

The Attorney General's Securities Division anticipates fraudulent investment schemes will rise as a result of the ongoing pandemic. "Scammers will be targeting investors, capitalizing on recent developments in the economy and preying on concerns about the regulated securities market," said Securities Commissioner Melanie Lubin. "Investors must remain vigilant to protect themselves."

In particular, fraudsters can be expected to develop schemes that falsely purport to raise capital for companies manufacturing personal protective equipment including surgical masks and gowns, producing ventilators and other medical equipment, distributing small-molecule drugs and other preventative pharmaceuticals, or manufacturing vaccines and miracle cures. The schemes often appear legitimate because they draw upon current news, medical reports and social and political developments.

Scammers also will seek to take advantage of concerns with the volatility in the securities markets to promote "safe" investments with "guaranteed returns" including investments tied to gold, silver and other commodities; oil and gas; and real estate. Investors also can expect to see "get rich quick" schemes that tout quickly earned guaranteed returns that can be used to pay for rent, utilities or other expenses. These schemes also target retirees and senior citizens, falsely claiming they can quickly and safely recoup any losses to their retirement portfolios.

The Attorney General encourages anyone who believes they have been the victim of a securities scam to contact the Securities Division at 410-576-6365 or by using the complaint form at http://www.marylandattorneygeneral.gov/Securities%20Documents/Scomplt.pdf

Retail investors must remain vigilant and protect themselves from new schemes tied to COVID-19 and recent economic developments. The Securities Division strongly suggests investors stay clear of anything sounding too good to be true, such as guarantees of high returns with no risk, and vet their investment professional about their licenses and registrations.

Investors should also contact the Securities Division with questions about any investment opportunity or the person offering it for sale before investing in the product. For more information, visit the Securities Division on the Attorney General's website http://www.marylandattorneygeneral.gov/Pages/Securities/default.aspx

INVESTOR BEWARE: Schemes to Watch for and How to Protect Yourself

Private placements and off-market securities. Scammers will take advantage of concerns with the regulated securities market to promote off-market private deals. These schemes will continue to pose a threat to retail investors because private securities transactions are not subject to review by federal or state regulators. Retail investors must continue to investigate before they invest in private offerings and independently verify the facts for themselves.

- **Gold, silver and other commodities**. Scammers may also take advantage of the decline in the public securities markets by selling fraudulent investments in gold, silver and other commodities that are not tied to the stock market. These assets may also be attractive because they are often promoted as "safe" or "guaranteed" as hedging against inflation and mitigating systematic risks. However, scammers may conceal hidden fees and mark-ups, and the illiquidity of the assets may prevent retail investors from selling the assets for fair market value. The bottom line is there really are no "can't miss" opportunities.
- **Recovery schemes**. Retail investors should be wary of buy-low sell-high recovery schemes. For example, scammers will begin promoting investments tied to oil and gas, encouraging investors to buy now so they can recognize significant gains after the price of oil recovers. Scammers will also begin selling equity at a discount, promising the value of the investments will significantly increase when the markets strengthen. Investors needs to appreciate the risks associated with any prediction of future performance and recognize that gains in the markets may not correlate with the profitability of their investments.
- **Get-rich-quick schemes**. Scammers will capitalize on the increased unemployment rate. They falsely tout their ability to quickly earn guaranteed returns that can be used to pay for rent, utilities or other expenses. They also target retirees and senior citizens, falsely claiming they can quickly and safely recoup any losses to their retirement portfolios. Remember: if it sounds too good to be true, it probably is.
- **Replacement and swap schemes**. Investors should be wary of any unlicensed person encouraging them to liquidate their investments and use the proceeds to invest in more stable, more profitable products. Investors may pay considerable fees when liquidating the investments, and the new products often fail to provide the promised stability or profitability. Advisors may need to be registered before promoting these transactions and legally required to disclose hidden fees, mark-ups and other costs.
- **Real estate schemes**. Real estate investments may prove appealing because the real estate market has been strong and low interest rates have been increasing the demand for housing. Scammers often promote these schemes as safe and secure, claiming real estate

can be sold and the proceeds can be used to cover any losses. However, real estate investments present significant risks, and changes to the economy and the real estate market may negatively impact the performance of the products.

How to Protect Yourself

The Securities Division provides the following guidance and tips to help investors avoid anticipated schemes seeking to take advantage of unsuspecting consumers and investors.

- Ask questions and research the investment and person offering it. Investors should always ask if the salesperson and the investment itself are properly licensed or registered. This information can be confirmed by the Securities Division at 410-576-6494. Investors also can check the <u>SEC's Investment Adviser Public Disclosure</u> database or <u>FINRA's</u> <u>BrokerCheck</u>. Avoid doing business with anyone who is not properly licensed.
- Don't fall for phishing scams. Phishing scams may be perpetrated by foreign or domestic parties claiming an association with the Centers for Disease Control and Prevention or the World Health Organization, or by individuals claiming to offer novel or expert medical advice or services. Con artists offering "opportunities" in research and development are scamming you. They may even be perpetrated by persons impersonating government personnel, spoofing their email addresses and encouraging their audience to click links or access malicious attachments. These emails may look real and sound good, but any unsolicited emails that have attachments and web links can point to dangerous websites and malicious attachments that can steal information from your computer, lock it up for ransom, or steal your identity. Don't click on it.
- There are no miracle cures. Scientists and medical professionals have yet to discover a medical breakthrough or have developed a vaccine or means to cure COVID-19. Not surprisingly, the vaccines being sold by online pharmacies are not real. You should not send money or make payments over the phone to anyone claiming they can prevent COVID-19, or purporting to have a vaccine or other preventive medicine.
- Avoid fraudulent charity schemes. White-collar criminals may pose as charities soliciting money for those affected by COVID-19. Before donating, you should independently verify any charity that is raising money for the sick or securing donations to help uninsured persons pay for medical treatment. You should also avoid online solicitations for cash and gift cards, as these schemes have become a popular way for scammers to steal money. Think with your head and not with your heart. If you want to donate to a cause, you should work with a legitimate, established organization.
- Be wary of schemes tied to government assistance or economic relief. The federal government may send checks to some members of the public as part of the economic stimulus effort. It will not, however, require the prepayment of fees, taxes on the income, or the advance payment of a processing fee or any other type of charge. Anyone who demands prepayment will almost certainly steal your money. And don't give out or verify any personal information either. Government officials already have your information. No federal or state government agency will call you and ask for personal information.



Consumer Alert: Tips to Avoid Coronavirus Stimulus Payment Scams

The federal government has begun making payments to individuals as authorized by the Coronavirus Aid, Relief, and Economic Security (CARES) Act. These are more commonly known as "stimulus" payments and will either be made directly into your bank account or you may be issued a check delivered by U.S. mail.

Unfortunately, there are also unscrupulous people taking advantage of these payments to try to scam others out of money or personal information. By understanding some basic information about these payments, we hope to help you avoid scammers and fraudsters.

- Residents of the United States who meet certain income limits are eligible to receive the stimulus payments. This means that not every U.S. resident is eligible, and therefore not every resident will receive a payment.
- The Internal Revenue Service (IRS) is the federal agency that is administering the payments. Communication from other agencies or entities that claim to be able to get you a stimulus payment is most likely a scam.
- The IRS will not call, text, email, or contact you on social media asking for personal or bank account information, even related to these stimulus payments.
- The IRS will mail a letter to your last known address about two weeks AFTER your payment providing information on how the payment was made and what to do if you didn't receive the payment. If you have questions about the legitimacy of this letter, you can visit <u>www.IRS.gov</u> for more information.
- If you are eligible for a payment and do not automatically receive a direct deposit or check, ONLY use the online form available through IRS.gov called "Non-Filers: Enter Payment Info" to provide personal information. Anyone asking for personal information through email, text, phone call, or social media is a scammer. (Most eligible individuals will receive a payment automatically without having to do anything. However, some individuals will need to complete this form to receive a payment).)
- You don't have to pay to get your stimulus money. The payment is not income and you do not have to pay any taxes now or in the future on this money.
- The IRS will not tell you to deposit your stimulus check then send them money back because they paid you more than they owed you. That's a fake check scam.
- Anyone that tells you must "act now" to get your stimulus payment is a scammer, especially if they are asking for your personal or financial information. If you don't receive a payment this year, you can also claim it by filing a 2020 tax return next year.

You should be able to find answers to all your questions about the stimulus payments on <u>www.IRS.gov</u>. But if you think you've been the victim of a scam, you can file a complaint with our Consumer Protection Division at <u>www.marylandattorneygeneral.gov</u>. If you believe your personal information and identity have been stolen or compromised, read our <u>ID Theft Guide</u> or email <u>IDtheft@oag.state.md.us</u> for guidance on recovering your identity.



Consumer Alert: Thousands of Eligible Marylanders are Missing Out on Stimulus Payments

Although around 160 million "stimulus" payments have been made to eligible U.S. residents, a <u>recent report</u> estimates that 12 million people, including 147,000 Marylanders, are missing out on receiving a payment. The payments yet to be distributed add up to around \$12 billion, \$157 million of which is owed to Maryland residents.

On March 27, 2020, the U.S. Congress passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act, which included payments (commonly known as "stimulus" payments) to eligible U.S. residents. These stimulus payments are intended to help residents deal with the effects of the COVID-19 pandemic, including a historic loss of jobs and income for millions of U.S. residents. Eligible adults can receive \$1,200 (\$2,400 for a married couple) and \$500 for each dependent child under 17 years old.

Most people eligible for these payments received them automatically because they filed federal income tax returns in 2018 or 2019 and included direct deposit information or receive certain federally administered benefits (such as Social Security, Supplemental Security Income, Railroad Retirement, or Veterans Affairs pension or disability benefits).

However, the estimated 12 million people—adults and children—who did not receive automatic payments include those who aren't required to file federal income tax returns due to their incomes and those who do not receive federally administered benefits like those listed above. This group of eligible payees are disproportionately people of color, who are hit hardest by both the economic and health effects of the pandemic.

These eligible payees must provide specific information to the IRS by submitting a 2019 tax return or using an online form called the IRS <u>"Non-Filer" tool</u> by **October 15, 2020** in order to receive a payment. Although the "Non-Filer" tool requires less information than a full tax return, for many eligible payees, using this form can be challenging as it requires internet access, an email address, a direct deposit account or an address to which the payment can be delivered.

Please share this information with anyone who believes they are eligible for a stimulus payment but has not yet received one.



Consumer Alert

Consumer Alert: Maryland District Court Resumes Debt Collection "Affidavit Judgment" Cases

Effective Monday, July 20, the District Court of Maryland once again started to hear debt collection "affidavit judgment" cases. In an affidavit judgment case, a creditor provides the court with an affidavit showing how much is owed. If the consumer does not file a notice of intention to defend and fails to appear in court on the date of the hearing, the court can enter a judgment without a hearing.

If you have been sued in court for a debt in an affidavit judgment case and receive a summons or hearing notice, you need to either file the "Notice of Intention to Defend" that is attached to the lawsuit or appear for the hearing. Do not ignore the lawsuit and scheduled hearing – **even if you believe you do not owe the debt or cannot afford to pay**. If you fail to either file a Notice of Intention to Defend or appear for your hearing, the Court may enter a judgment against you in the case.

Some courts are offering remote hearings by video or phone. If you are interested in appearing remotely on the affidavit judgment date, you should contact the <u>clerk of the court</u> where the action is pending.

If you receive a summons or hearing notice and need assistance, you may contact the Court's Self Help Centers at 410-260-1392 or <u>https://mdcourts.gov/selfhelp</u>.



Consumer Alert

Alert: Maryland Businesses Receiving Fake "2020 Certificate of Good Standing Request Form" Letter; Same Scam Letter Circulated in Late 2019

The Office of the Attorney General has received information that businesses in Maryland have been receiving a letter entitled "2020 Certificate of Good Standing Request Form" that requests a fee in exchange for a letter of good standing with an "official seal of the Secretary of State." This letter is a SCAM. This same scam letter was circulated in late 2019.

The scam letter asks the recipient to send a check or money order to an entity named "MD Certificate Service" in Annapolis, MD in exchange for an "elective Maryland Certificate of Good Standing." The letter goes to great lengths to look official with a "document number" and a barcode, and includes a customer service phone number of 1-855-222-3322.

Some business entities in Maryland are required to have a certificate of good standing, but not from the Secretary of State. An official certificate of good standing is available from the Maryland Department of Assessments and Taxation for a nominal fee.

If you receive this scam letter, do NOT send them any money. You can report the letter to the Maryland Secretary of State, the Federal Trade Commission (FTC) at <u>www.ftccomplaintassistant.gov</u>, or the United States Postal Inspection Service at <u>www.uspis.gov</u> or 1-877-876-2455.



Consumer Alert: Cyberthieves Are Posing as Major Companies in Phishing Schemes

Have you received an unexpected or unsolicited email, phone call, or text from a major company like Amazon, Google, or Apple? Before you click on the email or respond to a text or phone call, know that it's probably a scam. These types of scams are on the rise, and scammers are trying harder than ever to trap victims, and they are becoming more aggressive.

Often, these emails/calls/texts will state something like:

- Your account has unusual/suspicious activity;
- Your account has been altered and needs your attention right away;
- You need to update your payment information; or
- You need to take some other action, usually "urgently."

Other times, you may receive what looks like an order confirmation, that may or may not include an attachment, for an item you didn't purchase.

A scam email or text will often ask you to click a link, open an attachment, or call a number to resolve whatever issue it says needs your attention. When people respond, they're often asked to purchase gift cards or visit a website (provided by the scammer) to input payment information to resolve the issue. But to be absolutely clear— you should <u>never</u> call any number, open any attachments, or visit any website one of these calls or emails tells you to. This is one of the most common ways these scammers can trap you. The link could send you to a malicious website or launch a virus into your computer or phone. Alternatively, it may ask you to "verify" or submit personal or financial information, but the scammers are really just stealing it.

If you get a phone call from a representative claiming to be from one of these major companies, please be aware that <u>they will rarely call you for any reason</u>. Our advice is to ignore these calls, or if you do pick up and the caller asks you to disclose or verify personal and financial information, hang up right away. Major companies like Amazon, Apple, and Google will not ask you for this information unless you have initiated the call. If your phone service allows it, you may wish to block the suspicious caller's number.

There are red flags that can tip you off that you're dealing with a scam email or text. It could contain poor grammar and/or spelling, or the content just seems strange or farfetched. If the email originated from a different account than the supposed company trying to contact you (for example, an email claiming to be from Apple would not have a sender email address ending in gmail.com), it may be fraudulent. Is the link embedded in an email actually the same as the text

that is displayed? For instance, if the link says <u>www.amazon.com</u>, but displays something completely different when you hover your cursor over it, it may be fraudulent. Finally, if you didn't sign up for text messages or alerts from a particular company, you should ask yourself why they would contact you that way.

If you do need to contact a company's customer support, go directly to the company's official website to see how they prefer you contact them.

If you do provide information or purchase gift cards at the request of these scammers, recovering your money will be very difficult. Remember, providing personal information also makes you vulnerable to identity theft. If you believe the scam may have originated in the United States, we recommend that you contact your local police department or State's Attorney's Office to determine if they can assist you in recovering any of your money.

If you believe this scam may have originated outside of the United States, we recommend that you contact the FBI at <u>www.fbi.gov</u> to determine if they can assist you in recovering any of your money. Alternatively, you may call the Baltimore office at 410-265-8080 or the National Headquarters in DC at 202-324-3000. This type of crime may also be reported to the Internet Crime Complaint Center at <u>www.ic3.gov</u>.

The best way to protect yourself from these types of scams is to know the red flags and trust your instinct if you suspect something is off. Don't answer suspicious calls, but if you do and suspect it's a scammer—hang up and block the caller's phone number. Delete suspicious emails and texts. If you do open them, do not click on any links, open any attachments, or call any of the numbers listed. You are your own best defense against these scams.



Consumer Alert

Scam Alert: Phony Mortgage Company Representatives are Targeting Marylanders

The Office of the Attorney General has recently been notified of scams involving individuals impersonating mortgage companies. Some of these scammers are calling existing customers of a mortgage company, claiming to be representatives of that company, and offering the customer a loan modification. The scammer may ask for your full name, address, date of birth, and even your social security number. They may tell you that you have to give them this information immediately in order to qualify for the loan modification.

In another scam, individuals posing as mortgage company employees may call and tell you that you need to make a payment, and they may ask for a debit card number, money order, or gift card (this is a major red flag—no legitimate company will ask you to buy gift cards to make payments).

Other scammers may tell you to stop payment on your existing mortgage to make "trial" payments to them instead. They generally provide very "official" looking paperwork for you to sign. Do not fall for any of these tactics—they are trying to steal your personal information or money, or both. <u>Under no circumstances should you ever stop payment on your mortgage.</u> If you fail to pay your mortgage to the company that legitimately holds your loan, you could default on your loan and possibly even lose your home.

Telephone scams are common, and sometimes it can be difficult to distinguish legitimate calls from scammers. The caller ID could display the name of a real mortgage company in hopes they can trick you into answering the phone, but this is a common tactic used by scammers called "spoofing." If you do receive a phone call that displays the name of your mortgage company, our advice is to ignore the call and let it go to voicemail. Do not call back the number that was displayed on your phone. You can then call the company's actual phone number—listed on their official website—to ask if they called you and for what reason. If they did not call you, block the suspicious caller's phone number from trying to reach you again. Never give personal information to a caller you do not know or on a call you did not initiate.

If you have divulged personal or financial information to someone who called you, and now suspect they may have been trying to scam you, call or email our Identity Theft Unit at 410-576-6491 or <u>idtheft@oag.state.md.us</u> to learn how to protect your identity and financial information.



Utility Shut-Off Notices Begin Again: What To Do if You Receive One

As of October 1, 2020, utility companies in Maryland may once again started sending utility shut-off notices to consumers. However, the Maryland Public Service Commission (PSC) has prohibited residential utility shut-offs, including gas, water, and electric services, from occurring until at least November 15, 2020. The 45-day window between a utility shut-off notice and the date that the shut-off can occur provides consumers the time to apply for financial assistance or work out a payment plan with the utility.

If you are behind in utility payments and received a utility shut-off notice, there are actions you can take to help avoid having your service disconnected. Immediately upon receipt of a shut-off notice, contact the utility to ask about extended payments plans, budget billing, or other measures to avoid service termination.

You may also apply for emergency assistance to pay the utility bills that are overdue. Information on energy assistance programs is available from these resources:

- Maryland PSC website (<u>https://www.psc.state.md.us/wp-content/uploads/Need-Helpwith-Paying-your-Bill-or-Have-a-Termination-Notice-1-2-19-revisions.pdf</u>)
- Office of Home Energy Programs in the Maryland Department of Human Services (https://dhs.maryland.gov/office-of-home-energy-programs/) or call 1 (800) 332-6347
- Fuel Fund of Maryland (https://fuelfundmaryland.org) or call (410) 235-9080
- Maryland 211 (<u>https://211md.org/211provider-utility-assistance</u>), call 2-1-1 or text My211MD to 898-211
- Maryland Office of People's Counsel (<u>http://www.opc.maryland.gov/Consumer-Corner</u>)

If you work out a payment plan with the utility or find financial assistance to pay off your pastdue bills, the PSC has ordered that your service will not be disconnected. Any payment plan you work out with a company regulated by the PSC is required to be, at minimum, a 12-month repayment plan. Furthermore, these utilities may not collect a down payment or deposit as a requirement of that repayment plan.

Please note that not all utilities are subject to the PSC's order, including some telecom providers (such as wireless telephone companies) as well as some water and sewer agencies. If you received a shut-off notice from a utility that is not regulated by the PSC, contact that utility immediately to see if they will work out a payment plan to avoid disconnecting your service.

Do NOT wait to reach out for help if you receive a shut-off notice. If you don't take any action to help avoid a termination, the utility may disconnect your service 45 days after they have given you notice.



Consumer Alert

Consumer Alert – Scammers Posing as MD Board of Elections to Obtain Social Security Numbers

The Attorney General's Consumer Protection Division has been notified that some voters have been called and asked to verify their Social Security Numbers in order to process their ballots. **This is a scam.** Do not give your Social Security Number (SSN) to anyone over the phone unless you initiated the call and know exactly why you are providing it - for example, if you call your bank and do not have your account number, the bank representative may ask you for your SSN.

The Maryland Board of Elections (or local board of elections) may call you if there is an issue with your ballot or voter registration - for example, if your signature is missing on your mail-in ballot return envelope. If they need to verify your identity, they may ask for the last four digits of your SSN, **but they will never ask for your full SSN**.

If someone calls you claiming to be from the Board of Elections and asks for your full SSN, they are trying to scam you. They may use this information to steal your money, other personal information, or identity. Hang up immediately and do not call the phone number back that appears on your caller ID. If you have any questions about your ballot, call your <u>local Board of Elections</u>.



Consumer Alert

Consumer Alert: Important Information on Retail Energy Suppliers

November 12, 2020 - Maryland law gives consumers the right to choose a third-party energy supplier and give the suppliers the green light to market directly to consumers. Many of these companies make promises that switching from a public utility such as BG&E or PEPCO will save you money or help the environment by offering "cleaner energy." These suppliers must have a license from Maryland's Public Service Commission (PSC), and comply with Maryland law and PSC regulations. But, unlike public utilities, the rates and fees of these third-party suppliers are not subject to review and regulation.

As a residential consumer, you receive your energy supply from the public utility unless you choose to switch to a third-party company. However, some of these companies use heavy-handed tactics to persuade you to switch, or — even worse — may actually try to deceive you into switching suppliers. Switching a consumer's utility supply service without their permission is called "slamming." In 2019, the PSC shut down SmartOne Energy for this practice, revoking its license and ordering them to pay a penalty. On October 7, 2020, following a complaint from the Maryland Office of People's Counsel (OPC), the PSC found a different company, Smart Energy, in violation of PSC law and regulations, and ordered refunds to SunSea consumers solicited by telephone.

The Attorney General's Consumer Protection Division has received multiple complaints of telephone solicitors and door-to-door salespeople engaging in tactics such as impersonating public utility representatives and asking to view consumers' energy bills. If someone claims to be representing a public utility and you are already a customer, they would never need you to show them your bill — they would already have that information! If you show your current utility bill to a representative of a third-party supplier, they can obtain all the information they need to switch you without your knowledge or permission.

Some consumers complain that they were offered better rates than the public utility, but were surprised to find bills that included higher rates or additional fees, making their final bills higher than before they switched. In fact, third-party suppliers often have variable rates, and may apply additional fees and contract termination fees.

Before committing to switching to a third-party energy supplier, be aware that the majority of Maryland consumers actually pay more over time. A 2018 report by the Abell Foundation, Inc., on behalf of the OPC, found that third-party supply customers paid higher rates over time than

those who stayed with standard offer service provided by the utilities. According to this report, between 2014 and 2017 Maryland consumers using third-party electricity supply paid \$255 million more than consumers using public utilities (this study excluded suppliers that sell only 100 percent renewable energy products).

If you choose to switch to a third-party energy supplier, be sure to read their terms and conditions very carefully so you fully understand their rates and fees, the length of the contract, and if you are able to cancel the contract and when, if you change your mind. And remember, in almost all phone and all door-to-door solicitations, the agent must give you a contract to sign and return to the supplier.

Be wary of the following if you are visited by a door-to-door utility salesperson. These are red flags that they may be trying to switch your utility without your permission or knowledge.

- They don't immediately identify themselves or what company they work for, or fail to display their credentials;
- They are wearing attire or badges that closely resemble those of your public utility;
- They claim to have been "authorized" by your public utility to review your bill to see if they can save you money;
- They ask to see a paper copy of your current bill or view it online; or
- They claim that your public utility is changing their billing structure and need to review your bill with you.

If you are visited (or called) by someone claiming to be representing a third-party energy supplier, you have the right to request information to review before you make a decision about switching. Don't let the representative pressure you into making a decision quickly. You may wish to review complaint reports about local retail energy suppliers, which can be viewed on the PSC's website at https://www.psc.state.md.us/retail-energy-supplier-complaint-reports/. You have the right to get your energy from a public utility or select an alternative supplier of your choice, but they may never switch you without your permission.

For more information, visit the OPC website at <u>www.opc.maryland.gov</u>, and look for "Retail Suppliers" in the Consumer Corner.