Consumer Alert: Important Information on Door-to-Door Sales Scams

BALTIMORE, MD (January 25, 2024) – The Maryland Attorney General's Office is offering tips to help people avoid door-to-door sales scams.

Door-to-door scams have been around for years. Scammers may disguise themselves as legitimate salespeople, but they have one goal – to trick consumers. They want to pressure people into providing personal information or purchasing goods or services that they do not want or need.

Common door-to-door imposter scams:

Water Filtration Scams – These scammers may pose as representatives of the Environmental Protection Agency (EPA) or some other organization or company that is providing a "free" service to community residents. They may conduct a home water test to demonstrate how "contaminated" your drinking water is. Then they will talk you into having a home water filtration system installed "for free." However, their real goal is to deceive you into signing a loan agreement that could leave you owing hundreds or thousands of dollars for a filtration system that you never needed.

Fake Solar Energy Providers – These imposters try to take advantage of consumers who are looking for sustainable power to fuel their homes by convincing them to sign "enrollment forms" or "applications" that allow the imposters to steal your personal information or commit other fraudulent activities.

Fake Utility Representatives – Fraudsters may pose as utility workers who need to get into your home to inspect a "utility emergency." Once inside, they may steal your property or personal documentation.

Third-Party Energy Supplier Scams – Maryland law gives consumers the right to choose a third-party energy supplier and gives these suppliers the ability to market directly to consumers.

However, deceiving a consumer into switching suppliers is called "slamming." When companies fail to provide consumers with accurate and complete information to help them make informed decisions, they could be violating the law.

Home Improvement Scams – Be wary of contractors who knock on your door offering low-cost repairs, home improvement projects, or who claim to have extra supplies left over from another project in your neighborhood. These scammers may be quick to disappear if you provide them with any type of payment upfront.

Helpful tips for protecting yourself against door-to-door seller scams:

- Research the business before agreeing to allow any work to be done in your home or on your property.
- Legitimate salespeople will identify themselves immediately and have a photo identification in sight. They will not use high-pressure sales tactics, and they will provide you with written information and the time you need to do your research and make an informed decision.
- Keep your front and back doors locked while talking with any salesperson.
- Before you sign ANYTHING, insist that the salesperson provide you – even if they claim the work is "free" – with a complete contract that includes the terms and conditions, contact information for the company, a detailed description of the work to which you are agreeing, and the total amount you'll have to pay and when it's due. Make sure you read these documents, including the fine print, before you sign them, and insist that they leave copies of your signed documents with you before they start any work.
- You should not sign electronic documents on a tablet without first being provided with the entire agreement to read. You should also demand that a copy of the contract be provided to you immediately after you sign it.
- Require that the salesperson provide you with a written quote. Scammers may give a verbal quote with a good price, but then they may demand more money before the job is finished – or they may never finish the work at all.
- Never pay in cash. If you suspect fraud after the transaction, you may be able to dispute charges with your credit card company or stop payment on a check. If you pay in cash, you are unlikely to get that money back if you are scammed.
- Know your rights:
    - **Licenses** - Home improvement contractors and salespersons are required to be licensed by the Maryland Home Improvement Commission. The contractor's license number, as well as the name and license number of the salesperson, should be printed on the contract that you are offered. Consumers can verify a license through the Home Improvement Commission's website, www.dllr.state.md.us/license/mhic.
    - **Deposits** - It is against the law in Maryland for contractors to accept more than one-third of the total contract price when they enter into home improvement contracts. If a contractor asks you for more than one-third, that is a warning sign that the contractor may be trying to scam you.
    - **Right to Cancel** - Under the Maryland Door-to-Door Sales Act, you have three business days to cancel a door-to-door sale, unless it is for home improvement work (then you have five business days). If it is for home improvement work and you are at least 65 years old, then you have seven days. If you are not provided

with a written notice explaining these rights, you should not do business with the seller.

- Remember: If someone knocks on your door and offers a deal that seems too good to be true, it likely is.

https://www.marylandattorneygeneral.gov/press/2024/012524CA.pdf

Alerta al Consumidor: Información Importante sobre las Estafas de Ventas Puerta a Puerta

BALTIMORE, MD (25 de enero de 2024) – La Oficina de la Procuraduría General de Maryland ofrece consejos para ayudar a las personas a evitar las estafas de ventas puerta a puerta.

Las estafas puerta a puerta existen desde hace años. Los estafadores pueden disfrazarse de vendedores legítimos, pero tienen un objetivo: engañar a los consumidores. Quieren presionar a las personas para que proporcionen información personal o compren bienes o servicios que no quieren o no necesitan.

Estafas comunes de impostores puerta a puerta:

Estafas de Filtración de Agua: estos estafadores pueden hacerse pasar por representantes de la Agencia de Protección Ambiental (EPA) o alguna otra organización o empresa que brinde un servicio "gratuito" a los residentes de la comunidad. Es posible que realicen una prueba de agua en el hogar para demostrar qué tan "contaminada" está su agua potable. Luego, lo convencerán para que instale un sistema de filtración de agua en el hogar "gratis". Sin embargo, su verdadero objetivo es engañarlo para que firme un contrato de préstamo que podría dejarlo debiendo cientos o miles de dólares por un sistema de filtración que nunca necesitó.

Proveedores Falsos de Energía Solar: estos impostores intentan aprovecharse de los consumidores que buscan energía sostenible para alimentar sus hogares convenciéndolos de que firmen "formularios de inscripción" o "solicitudes" que permiten a los impostores robar su información personal o cometer otras actividades fraudulentas.

Representantes Falsos de Servicios Públicos: los estafadores pueden hacerse pasar por trabajadores de servicios públicos que necesitan ingresar a su hogar para inspeccionar una "emergencia de servicios públicos". Una vez dentro, pueden robar sus pertenencias o documentación personal.

Estafas de Proveedores de Energía de Terceros: la ley de Maryland otorga a los consumidores el derecho de elegir un proveedor de energía de terceros y les brinde a estos proveedores la capacidad de comercializar directamente a los consumidores. Sin embargo, engañar a un consumidor para que cambie de proveedor se llama "slamming". Cuando las empresas no proporcionan a los consumidores información precisa y completa para ayudarlos a tomar decisiones informadas, podrían estar violando la ley.

Estafas de Mejorar el hogar: tenga cuidado con los contratistas que llaman a su puerta ofreciendo reparaciones de bajo costo, proyectos de mejorar el hogar o que afirman tener suministros adicionales sobrantes de otro proyecto en su vecindario. Estos estafadores pueden desaparecer rápidamente si les proporciona cualquier tipo de pago por adelantado.

Consejos útiles para protegerse contra las estafas de vendedores puerta a puerta:

- Investigue el negocio antes de aceptar permitir que se realice cualquier trabajo en su hogar o en su propiedad.
- Los vendedores legítimos se identificarán de inmediato y tendrán una identificación con foto a la vista. No utilizarán tácticas de venta de alta presión y le proporcionarán información escrita y el tiempo que necesita para investigar y tomar una decisión informada.
- Mantenga las puertas delanteras y traseras cerradas con llave mientras habla con cualquier vendedor.
- Antes de firmar CUALQUIER COSA, insista en que el vendedor le proporcione, incluso si afirma que el trabajo es "gratuito", un contrato completo que incluya los términos y condiciones, la información de contacto de la empresa, una descripción detallada del trabajo que está aceptando y la cantidad total que tendrá que pagar y cuándo debe pagarse. Asegúrese de leer estos documentos, incluida la letra pequeña, antes de firmarlos, e insista en que le dejen copias de sus documentos firmados antes de que comiencen cualquier trabajo.
- No debe firmar documentos electrónicos en una tableta sin antes que se le proporcione el acuerdo completo para leer. También debe exigir que se le proporcione una copia del contrato inmediatamente después de firmarlo.
- Exija que el vendedor le proporcione una cotización por escrito. Los estafadores pueden dar una cotización verbal con un buen precio, pero luego pueden exigir más dinero antes de que se termine el trabajo, o es posible que nunca terminen el trabajo.
- Nunca pague en efectivo. Si sospecha de fraude después de la transacción, es posible que pueda disputar los cargos con la compañía de su tarjeta de crédito o suspender el pago de un cheque. Si paga en efectivo, es poco probable que recupere ese dinero si lo estafan.
- Conozca sus derechos:
    - **Licencias** : los contratistas y vendedores de mejorar el hogar deben tener una licencia de la Comisión de Mejoras para el Hogar de Maryland. El número de licencia del contratista, así como el nombre y el número de licencia del vendedor, deben estar impresos en el contrato que se le ofrece. Los consumidores pueden verificar una licencia a través del sitio web de la Comisión de Mejoras para el Hogar, www.dllr.state.md.us/license/mhic.
    - **Depósitos** : es ilegal en Maryland que los contratistas acepten más de un tercio del precio total del contrato cuando celebran contratos de mejoras para el hogar. Si un contratista le pide más de un tercio, es una señal de advertencia de que el contratista puede estar tratando de estafarlo.

    - **Derecho a cancelar**: según la Ley de Ventas Puerta a Puerta de Maryland, tiene tres días hábiles para cancelar una venta puerta a puerta, a menos que sea para trabajos de mejorar el hogar (entonces tiene cinco días hábiles). Si es para trabajos de mejorar el hogar y tiene al menos 65 años, entonces tiene siete días. Si no se le proporciona una notificación por escrito que explique estos derechos, no debe hacer negocios con el vendedor.
- Recuerda: si alguien llama a tu puerta y te ofrece una oferta que parece demasiado buena para ser verdad, es probable que lo sea.

https://www.marylandattorneygeneral.gov/press/2024/012524CA_es.pdf

FOR IMMEDIATE RELEASE

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

Alert Issued to Consumers to Beware of Scam Election Calls

BALTIMORE, MD (March 5, 2024) – The Maryland Attorney General's Office is offering information to help people detect and avoid scam election calls. This alert was issued to all consumers who have subscribed to receive consumer information from our office. Consumers can subscribe to this list here: https://public.govdelivery.com/accounts/MDAG/subscriber/new.

Election call scams are a serious threat to the fairness and trustworthiness of elections, even posing a substantial threat to democracy itself. These scams usually involve robocalls that impersonate real political campaigns or candidates. The goal of these calls is to deceive you, manipulate your choices, and potentially disrupt the entire voting process. *Any call that directs you NOT to exercise your right to vote is a scam.*

Robocalls are often from scammers who want to steal your money or your identity, but election call scams are often trying to persuade you to perform, or not perform, a certain action. One of the most appalling scams occurs when fraudsters try to convince you to not exercise your right to vote. If you answer a phone call and hear a celebrity's or politician's recorded voice, keep in mind that this voice could have been faked by artificial intelligence (AI) and may not be who you think it is.

Companies that use AI to impersonate government officials may be violating the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, and other state consumer protection laws, according to the Federal Communications Commission.

The Maryland Office of the Attorney General fights to stop illegal robocalls and enforces consumer protection laws against robocalling scammers. In 2012, our office won a judgment of over $1 million against a company that violated the TCPA by placing robocalls to 112,000 Democrat voters. These calls suggested to voters that they did not have to vote in that election because Democrat candidates had already won. In this case, the Court found that "the purpose of the message was to suppress the votes of the largely African American and Democratic populations in Baltimore City and Prince George's County."

Recently, The Anti-Robocall Multistate Litigation Task Force (Task Force), which includes the Maryland Attorney General's Office, issued a warning letter to a company that allegedly sent New Hampshire residents scam election robocalls that mimicked President Joe Biden's voice to discourage voters from voting in New Hampshire's January primary election.

The Task Force of 51 bipartisan Attorneys General investigates and takes legal action against those responsible for routing illegal robocalls into and across the United States. Our office and the other members of the Task Force sued another company suspected of making millions of illegal robocalls to Marylanders. To read our press release on that lawsuit, click here: https://www.marylandattorneygeneral.gov/press/2023/052323a.pdf.

If you think you or somebody you know has received a scam election call, contact our office's Consumer Protection Division at 410-528-8662 with as much information as you are able to provide, including the date and time of the call, the number and name on the caller ID, and the subject of the call.

###

https://www.marylandattorneygeneral.gov/press/2024/030524CA.pdf

CONSUMER ALERT: Marylanders Should Be Wary of Deceptive Online Sports Betting Companies and Scams

BALTIMORE, MD (May 17, 2024) – Preakness Weekend 2024 has arrived and Attorney General Anthony Brown is urging Marylanders again to be aware of deceptive online sports betting companies. This alert was issued to all consumers who have subscribed to receive consumer information from our office. Consumers can subscribe to this list here: https://public.govdelivery.com/accounts/MDAG/subscriber/new.

The online sports betting industry, which launched in Maryland in 2022, also operates through mobile apps, has enticed bettors with aggressive marketing, such as so-called "risk-free" bets. Enticements and complicated "deals" may end up costing consumers more money than they were planning to spend in the first place. Online gambling is also a target for cybercriminals looking to defraud unsuspecting bettors.

In Maryland, the only legal wagering on sporting events is through sports wagering operators that are licensed and regulated by the Maryland Lottery and Gaming Control Agency (MLGCA) (www.mdgaming.com/maryland-sports-wagering/). Marylanders can also legally participate in online fantasy sports competitions that are offered by fantasy competition operators who are registered with the MLGCA (www.mdgaming.com/ancillary-responsibilities/fantasy-competitions/).

Attorney General Brown offers the following tips to protect consumers from misleading information peddled by online sports betting platforms:

- Learn what other users are saying about the platform: Check consumer reviews and ratings with the Better Business Bureau (www.BBB.org). The BBB complaints are often detailed and include responses from the platforms.
- Read the fine print! Especially on all promotions and bonus money.
    - With respect to "risk-free" bets, for example, those funds may only be credited back to the consumer to use again with the platform, not as a refund of the money the consumer initially invested.

    - Platforms sometimes require users to gamble their own money before accessing any bonus they advertised.
    - Some platforms may restrict the games for which consumers can use promotional money or have additional restrictions that are only listed in the fine print.
- Read all the conditions placed by the platform that may limit how and when bettors are able to cash out their winnings, or if the sportsbook will penalize bettors – such as freezing accounts –for certain activities and strategies the bettor may use on their platform to increase their chances of winning.
- Remember that there is no such thing as a completely risk-free bet, or free money, when it comes to gambling, despite what may be implied by an ad.

To protect against fraudulent platforms and scammers looking to steal money and financial and personal information, consumers should follow these tips:

- The internet is flooded with fraudulent sports betting websites. Make sure that you are using the official websites of established sportsbooks that have been approved by Maryland's Lottery and Gaming Control Agency.
- Ignore online gambling pop-up ads and unsolicited emails, text messages, or social media messages. Even if these look like they are coming from a legitimate sportsbook, they could be linking you to a fraudulent website instead.
- Report suspected scams to our Consumer Protection Division at 410-528-8662, or the Federal Bureau of Investigation at https://tips.fbi.gov/.

Remember that gambling causes financial losses and should only be done in moderation. Maryland residents seeking help with a gambling problem are encouraged to call 1-800-GAMBLER, a free and confidential helpline that is available 24 hours a day and is staffed by peer counselors and professionals from the Maryland Center of Excellence on Problem Gambling, a division of the State of Maryland's Behavioral Health Administration. Additional information on problem gambling resources is available by visiting www.mdgamblinghelp.org.

###

https://www.marylandattorneygeneral.gov/press/2024/051724CA.pdf

CONSUMER ALERT: Scammers Targeting E-ZPass Users in Fake Texts

BALTIMORE, MD (May 28, 2024) – Attorney General Anthony G. Brown is warning consumers about scam texts falsely claiming to represent a road toll collection service asserting that you owe money for unpaid tolls. The scam text looks similar to the example displayed below:

> Maryland Toll Services: We've noticed an outstanding toll amount of $12.51 on your record. To avoid a late fee of $50.00, visit https://sunspasstolls.com to settle your invoice.

Do not pay any money or reveal any personal information to any person or group that contacts you through a text about a toll debt.

If you receive one of these texts, the Attorney General recommends that you:

- Do NOT click on any links in the text.
- File a complaint with the FBI Internet Crime Complaint Center (IC3) at www.ic3.gov, and be sure to include:
  - The phone number from which the text originated; and
  - The website listed in the text.
- Check your account using the toll service's legitimate website. For Maryland E-ZPass, this website is https://driveezmd.com/.
- Contact the toll service's customer service phone number. Maryland E-ZPass' customer service number is 1-888-321-6824.
- After doing the above, delete any texts like this that you receive.

If you have received a text like this and paid the texter any amount of money or revealed any personal information, follow these steps:

- Contact the company that facilitated the funds transfer to see if you can stop the payment.

- Contact the Attorney General's Identity Theft Unit to learn how to protect yourself in case the scammers try to use your personal information and how to recover if you are impacted financially.
- Contact your local law enforcement department to report the theft.
- Report the incident to the Office of the Attorney General or the Federal Trade Commission.

This alert was issued to all consumers who have subscribed to receive consumer information from our office. Consumers can subscribe to this list here: https://public.govdelivery.com/accounts/MDAG/subscriber/new.

###

https://www.marylandattorneygeneral.gov/press/2024/052824CA.pdf

CONSUMER ALERT: Spotting and Avoiding Imposter Scams

BALTIMORE, MD (May 31, 2024) – Attorney General Anthony G. Brown is warning consumers about the growing threat of imposter scams, with scammers using sophisticated technologies to deceive the people they target. These scammers impersonate trusted figures, such as government officials, official representatives from banks, law enforcement, tech support agents, or even family members or friends, to steal your money or personal information.

A note about artificial intelligence (AI): Voices generated by AI are often used in scams. These are fake voices created by computers to sound like real people. Scammers use this technology, mimicking voices and even speech patterns, to trick people into believing they are talking to someone they know or trust. This makes it very difficult to tell the difference between a legitimate call and a scam.

The bottom-line is no matter what kind of technology or trickery these fraudsters use, you can learn how to effectively spot and avoid all kinds of imposter scams. The Attorney General's Office is here to help you do this.

Common Imposter Scam Types

- Government Imposters: For example, the caller may claim to be from the IRS, Social Security Administration, or Medicare, and threaten you with fines or arrest.
- Family or Friend Imposters: A scammer may pretend to be a relative or friend in distress who needs money urgently.
- Tech Support Scams: Fake tech support agents will claim your computer has a virus and demand access or payment for unnecessary repairs.

Recognize Imposter Scam Red Flags

- Unsolicited Calls or Emails: Be cautious of unexpected contact from individuals claiming to be from reputable organizations. Scammers often pretend to be from the IRS, Medicare, or Social Security.
- Urgency and Fear Tactics: Scammers often create a sense of urgency, claiming that immediate action is required to avoid severe consequences, such as legal action, arrest, fines, or account suspensions. They may tell you that they are offering a limited-time deal to push you into making hasty decisions. Or they may claim there is a health emergency, and you must act immediately to protect a loved one.
- Requests for Personal Information: Be cautious if the caller asks for sensitive information, such as Social Security numbers, banking details, or remote access to your computer.
- Payment Requests: Requests for payment using gift cards, wire transfers, or cryptocurrency are major red flags.

How to Verify Someone's Identity

- Contact the Organization: If you receive a suspicious call, hang up, and then contact the organization or agency directly using official contact information found on their website or through trusted directories.
- Ask Questions: Always verify the caller's identity by asking questions only the real person would know. Scammers often struggle to answer detailed questions or provide verifiable information. Hang up and call back using a known, trusted number for the individual claiming to be on the phone.
- Use a Code Word: Establish a code word with friends and family members that only they would know and use in case of an emergency.

Protect Yourself

- Hang Up: If you suspect a scam, hang up immediately. You do not need to be polite to scammers.
- Never Share Personal Data: Never share personal information, such as Social Security numbers or bank details, over the phone or through email unless you are certain of the recipient's identity.
- Stay Calm and Don't Panic: Scammers rely on fear. Take your time to think and verify before acting on any request.
- Talk to Someone You Trust: Before taking any action based on an urgent call, consult with a trusted family member or friend to gain their perspective.

Report Suspected Scams

You can report suspected imposter scam calls or emails to:

- The Attorney General's Consumer Protected Division at www.marylandattorneygeneral.gov (file a general complaint)
- The Federal Trade Commission (FTC) at www.ftc.gov/complaint
- AARP Fraud Watch Network at www.aarp.org/fraudwatchnetwork

- The FBI at www.IC3.gov.

If a scammer does steal money from you, contact your local police department to report the theft. If the scam involved transferring funds, immediately contact the financial institution from which you transferred funds and ask that the transfer be reversed.

Identity Theft

If you suspect that an imposter scammer has obtained your personal information and could steal your identity, our Consumer Protection Division has tools available to help you address it. Visit www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx for helpful tips and steps you can take to protect yourself or recover from identity theft, or call our Identity Theft Program at 410-576-6491 or send an email to idtheft@oag.state.md.us.

This alert was issued to all consumers who have subscribed to receive consumer information from our office. Consumers can subscribe to this list here: https://public.govdelivery.com/accounts/MDAG/subscriber/new.

###

https://www.marylandattorneygeneral.gov/press/2024/053124CA.pdf

ANTHONY G. BROWN, MARYLAND ATTORNEY GENERAL

PRESS RELEASE

FOR IMMEDIATE RELEASE

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

Credit Monitoring and Identity Theft Protection Resources Available to Consumers Following Change Healthcare (a Unit of UnitedHealth) Cyberattack

BALTIMORE, MD (July 11, 2024) – Attorney General Anthony G. Brown is alerting Marylanders about a data breach experienced in February 2024 by Change Healthcare, the nation's biggest electronic data clearinghouse. The clearinghouse, a unit of UnitedHealth, is used by tens of thousands of doctor's offices, hospitals, pharmacies, and insurers to verify insurance, confirm pre-authorization of procedures or services, exchange insurance claim data, and perform other administrative tasks essential to the delivery of healthcare.

Attorney General Brown is encouraging Marylanders to take steps to protect themselves, including taking advantage of the free credit monitoring and theft protection that is being offered in connection with the data breach.

The February cyberattack interrupted operations for thousands of doctor's offices, hospitals, and pharmacies. It also resulted in sensitive health and personal data being leaked onto the dark web—a hidden portion of the internet where cyber criminals buy, sell, and track personal information. The actual number and identity of affected patients are currently unknown; however, Change Healthcare has publicly stated that the data breach could impact up to one-third of all Americans. Given the significance of the breach and the fact that the company has not yet notified individuals if their data was impacted, Attorney General Brown is publicizing the breach and resources, including the offer that Change Healthcare has provided to the public.

Change Healthcare is offering ALL Maryland residents who believe they may have been impacted free credit monitoring and identity theft protections for two years. The dedicated website and call center will not be able to provide details about whether an individual's data was impacted, but it can guide them in obtaining free credit monitoring and identity theft protections. Marylanders should assume their data was included in the breach and consider signing up for the free credit monitoring and identity theft protections by calling or visiting Change Healthcare:

- For information, visit Change Healthcare Consumer support page - UnitedHealth Group.
- To enroll in credit monitoring through IDX, use the link at Change Healthcare Consumer support page - UnitedHealth Group or call **1-888-846-4705.**
- For additional support from Change Healthcare, call **1-866-262-5342.**

Marylanders should be aware of potential warning signs that someone is using their medical information. The signs include:

- A bill from their doctor for services they did not remember receiving;
- Errors in their Explanation of Benefits statement, like services they never received or prescription medications they do not take;
- A call from a debt collector about a medical debt they do not owe;
- Medical debt collection notices on their credit report that they do not recognize;
- A notice from their health insurance company indicating they have reached their benefit limit when they haven't; or
- They are denied insurance coverage because their medical records show a pre-existing condition they do not have.

Any Marylander who receives a suspicious email, phone call, or text from their healthcare provider or insurance company should refrain from sharing their personal information until they have separately confirmed the caller or writer is their actual doctor or insurance company.

If Marylanders are concerned that their data may have been impacted but prefer not to use the free resources provided by Change Healthcare, they can also consider **freezing their credit.**

A credit freeze prevents creditors—such as banks or lenders—from accessing an individual's credit reports. This will stop identity thieves from taking out new loans or credit cards in a consumer's name because creditors will not approve their loans or credit requests if they cannot first access their credit reports.

When an individual freezes their credit with each bureau, the bureaus will send them a personal identification number (PIN). The individual can then use that PIN to temporarily unfreeze their credit if they want to apply for a loan or credit card.

Marylanders who choose to freeze their credit should do it by contacting each bureau—Experian, Equifax, and TransUnion—on the internet or by phone:

- 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

For more information about protecting your privacy, please review Attorney General Brown's How to Protect Your Privacy guide, which is available here.

Joining Attorney General Anthony G. Brown in sharing these consumer protection resources is a bipartisan group of attorneys general from across the country.

This alert was issued to all consumers who have subscribed to receive consumer information from our office. Consumers can subscribe to this list here: https://public.govdelivery.com/accounts/MDAG/subscriber/new.

###

https://www.marylandattorneygeneral.gov/press/2024/071124CA.pdf

ANTHONY G. BROWN, MARYLAND ATTORNEY GENERAL

PRESS RELEASE

FOR IMMEDIATE RELEASE

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

CONSUMER ALERT: Avoiding Fraudulent Charities and Scams While Donating to Hurricane Relief

BALTIMORE, MD (October 17, 2024) – Attorney General Anthony G. Brown is warning consumers to beware of fraudulent charities and scams when donating to hurricane relief efforts. This alert was issued to all consumers who have subscribed to receive consumer information from our office. Consumers can subscribe to this list here: https://public.govdelivery.com/accounts/MDAG/subscriber/new.

As many states across the Southeast are facing a difficult recovery from the unprecedented devastation caused by Hurricanes Helene and Milton, many individuals are eager to help those affected by making donations. Unfortunately, scam artists often take advantage of disasters like these to set up fake charities and exploit your goodwill, so you'll want to be on the lookout for fraudulent charities and other scams.

Before donating any money to a charitable organization, check to see if the charity in which you are interested is registered with the Maryland Secretary of State's Public Registry. Donate to **well-known national or local charities** with experience in disaster relief. Several websites (such as GuideStar and Charity Navigator) provide information on an organization's financials, mission statements, and more. This information may help you decide how to divide up your giving. Bogus charities frequently use names and logos that are slightly changed but resemble well-known, legitimate organizations.

Some strategies you want to keep in mind to protect yourself from fraud include:

- Never agree to give money over the phone or to a door-to-door solicitor. Ask the caller or solicitor for written information about the charity and read it before making your decision.
- Avoid high-pressure and time-sensitive tactics, such as solicitors who are urging you to make an immediate donation. Even if the charity has an urgent need for money, the need will still exist after you have vetted the organization to make sure it's legitimate.

- Be wary about clicking on requests for donations found in emails, on a third-party website, or on social media. Scammers frequently lure consumers through social media or emails to fake websites, which are set up to steal personal and/or financial information or to release malware onto your computer.
- Before donating to a particular organization, search the charity's name online with terms like "scam" or "review" to see what, if any, experiences others have had with it.
- Don't respond to requests for prepaid credit cards, gift cards or bitcoin. Someone asking for donations in prepaid credit cards, gift cards, or bitcoin is most likely a scammer.
- Do not agree to send money through a courier or wire. Legitimate charitable organizations do not send couriers to pick up contributions.

Finally, remember that a legitimate organization should be able to clearly explain how your donation will be used and provide you a receipt for tax purposes.

Your generosity can make a real difference, but it's essential to stay vigilant. By taking these precautions, you can ensure your contributions genuinely help the victims of Hurricane Helene and Hurricane Milton.

Read more about charitable donations in our "Keeping Your Eyes Open When Donating to Charities" Consumer's Edge.

###

https://www.marylandattorneygeneral.gov/press/2024/101724CA.pdf

ANTHONY G. BROWN, MARYLAND ATTORNEY GENERAL

PRESS RELEASE

FOR IMMEDIATE RELEASE

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

CONSUMER ALERT: Office of Attorney General, MVA, Warn Consumers about Purchasing Flood-Damaged Cars

BALTIMORE, MD (November 25, 2024) – Attorney General Anthony G. Brown and the Maryland Department of Transportation Motor Vehicle Administration (MVA) are partnering to warn consumers in the market for a used car to be aware of flood damaged vehicles originating from states recently impacted by hurricanes and flooding. This alert was issued to all consumers who have subscribed to receive consumer information from our office. Consumers can subscribe to this list here: https://public.govdelivery.com/accounts/MDAG/subscriber/new.

"Marylanders shouldn't spend their hard-earned money on a car that is unsafe or doesn't work," said **Attorney General Anthony G. Brown**. "Buying a car is a significant investment of time and money. We urge everyone to do their due diligence before making a such a purchase."

"The MVA has implemented programs – such as the National Motor Vehicle Title Information System - which is designed to protect consumers from fraud and unsafe vehicles from being resold, however customers must still do their due diligence when purchasing a used vehicle," **said Motor Vehicle Administrator Chrissy Nizer**. "Vehicles that have flood damage may look good on the surface, but the irreversible damage may not always be visible. It's incredibly important to do your research and know what to look for."

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 that is loose, stained, doesn't match, 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.

Many signs of flood damage are not always obvious, such as water damage compromising the car's computer and safety mechanisms, including airbag sensors. The MVA and the OAG have the following tips for consumers looking to buy a vehicle:

- Take the time to inspect the vehicle. Check the engine for a high-water mark on the engine block or radiator. Look for rust or corrosion on wires and other components under the hood. Don't forget to check the trunk and under the spare tire for any water marks.

- Shop at a licensed dealer. Flood damaged vehicles often end up at auctions or sold by "curb stoners." Curb stoning is a way for unscrupulous sellers to avoid laws. They may pose as a private seller or through an online service. Not all private sellers are curb stoning, but you should check thoroughly before making the purchase.
- Check the Vehicle Identification Number (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 here. There are several other resources that can provide a detailed history of the car including:
  - Carfax (www.carfax.com);
  - Auto Check (www.autocheck.com); and
  - Consumer Guide (www.consumerguide.com).
- Consider taking the car to a qualified mechanic to inspect the vehicle thoroughly.

The MVA receives real-time alerts through the National Motor Vehicle Title Information System (NMVTIS). All jurisdictions in the continental United States participate in NMVTIS by contributing title and brand information, including flood damaged vehicles. When a customer titles and registers a vehicle in Maryland, their vehicle information number and title number is run through NMVTIS to ensure information is accurate and up to date. For more information about purchasing a vehicle in Maryland, visit MVA's website here.

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

###

https://www.marylandattorneygeneral.gov/press/2024/112524CA.pdf