AG Nessel Recognizes Utility Scam Awareness Day, Shares Ingredients of Impersonation Tactics

Nessel's <u>Utility Imposter Scams Consumer Alert</u> educates consumers on ways bad actors will impersonate utility employees in an effort to obtain money or personal information from an unsuspecting customer.

Utility Scam Awareness Day was created by <u>Utilities United Against Scams (UUAS)</u>, a consortium of 145 U.S. and Canadian electric, water, and natural gas companies and their respective trade associations.

"We know there's a direct correlation between entering the winter months and a rise in utility imposter scams," Nessel said. "Don't fall for scammers who contact you with a demand for money or personal information in exchange for keeping your service going. If you have any doubt about a caller, or suspect the call may be fraudulent, contact your utility using the phone number on your most recent bill and ask to speak to a customer service representative. You should also file a complaint with my office."

Last month, Nessel reissued her <u>Government Imposter Scams Consumer Alert</u>, which is the same scam approach, only the bad actors use legitimate government references and the threat of government action to trick individuals into taking action that facilitates theft. The alert was reissued after the Department of Licensing and Regulatory Affairs learned licensees were being targeted.

Just this week, <u>Michigan State Police warned residents</u> of scam calls where con artists are spoofing their phone numbers, making their numbers appear as MSP numbers on caller ID. Spoofing is a way in which bad actors can appear to be a legitimate entity when conducting an impersonation scam.

Signs of potential imposter scam activity:

- Threat to disconnect the utility or of another action against the individual: Scammers may
 aggressively tell a customer their utility bill is past due, and service will be disconnected—
 usually within an hour—if a payment is not made. If the scammer is impersonating law
 enforcement, the threat would likely be an arrest.
- Request for immediate payment: Scammers may instruct the person to purchase a prepaid card, cryptocurrency, or to send funds via a mobile app to make a bill payment or pay off a debt. If the scammer is impersonating law enforcement, the payment would be proposed as the only way to avoid arrest.

How utility customers can protect themselves:

- Customers should never purchase a prepaid card to avoid service interruption or pay a debt supposedly owed. Utility companies do not specify how customers should make a bill payment and always offer a variety of ways to pay a bill.
- If someone threatens immediate service interruption, customers should be aware. Customers
 with past due accounts receive multiple advanced notices, typically by mail and in their regular
 monthly bill. Utilities will never notify of a disconnection in one hour or less.
- If customers suspect someone is trying to scam them, they should hang up, delete the email, or shut the door. The utility should be contacted immediately at the number on the most recent

- monthly bill or on the utility's official website, not the phone number the scammer provides. If customers ever feel that they are in physical danger, they should call 9-1-1.
- If you've mistakenly provided bank account or credit card information to someone you suspect might have been an impostor, call your bank or credit card company immediately.

The Department of Attorney General provides <u>a library of resources for consumers to review anytime on</u> <u>a variety of topics</u>.

Your connection to consumer protection is just a click or phone call away. <u>Consumer complaints can be filed online at the Attorney General's website</u>, or by calling 877-765-8388.