State of Michigan
Attorney General Dana Nessel

FOR IMMEDIATE RELEASE:
Friday, April 1, 2022

AG Nessel Reissues Consumer Alert Following Verizon Smishing Warning

LANSING – Michigan Attorney General Dana Nessel is sharing reminders from her Text Message Scams: Smishing Consumer Alert as Verizon customers are warned about scam messages from their own number.

Smishing is when scammers send text messages pretending to be from trusted sources. The goal is to get targets to respond with personal information like passwords and credit card details or to click on links that install malware. It is just like phishing that uses emails; instead smishing uses texts.

The company told The Verge earlier this week, "Verizon is aware that bad actors are sending spam text messages to some customers which appear to come from the customers' own number. Our team is actively working to block these messages, and we have engaged with US law enforcement to identify and stop the source of this fraudulent activity. Verizon continues to work on behalf of the customer to prevent spam texts and related activity."

The scam text reads like this: "Verizon Free Msg: Latest bill processed. Thanks, [MyName]! Here's a little freebie for you: f1smk.exy/XXXXXXXX"

In response, Nessel wants to remind residents of ways to protect your number and information:

- **Don't** share your phone number unless you know the person or organization well.
- **Don't** assume a text is legitimate because it comes from a familiar phone number or area code. Spammers use caller ID Spoofing to make it appear the text is from a trusted or local source.
- **Don't** provide personal or financial information in response to the unsolicited text or at a website linked to the message.
- **Don't** click on links in suspicious text; they could install malware on your device or take you to a site that does the same.
- **Don't** reply, even if the message says you can "text STOP" to avoid more messages. That tells the scammer or spammer your number is active and can be sold to other bad actors.
- **Never** follow a text's instructions to push a designated key to opt out of future messages.

"A common smishing tactic is to send a text warning about a fake problem with one of your accounts and ask for your information," Nessel said. "Or some scammers will pitch offers too good to be true or

even promise free gift cards or trips in order to convince the recipient to click or respond. If this happens, ignore it. It could put malware on your device and lead to identity theft."

If you are an AT&T, T-Mobile, Verizon, Sprint or Bell subscriber, you can report spam or smishing texts to your carrier by copying the original text and forwarding it to 7726 (SPAM), free of charge.

If you cannot use 7726, then report smishing texts to your mobile service provider and the Federal Communications Commission (FCC).

The Department provides a library of resources for consumers to review anytime on a variety of topics.

Your connection to consumer protection is just a click or phone call away. Consumer complaints can be filed online at the Attorney General's website, or if you have questions call 877-765-8388.