T-Mobile

Testimony to the House Energy, Utilities and Telecommunications Committee
Summary of T-Mobile's Customer Protection against Unwanted Robocalls
February 18, 2020
Stacey Briggs representing T-Mobile

Chairman Seiwert and members of the House Energy, Utilities and Telecommunications Committee. My name is Stacey Briggs. I am the Sr. Manager of State Legislative Affairs for T-Mobile. T-Mobile is the industry leader in protecting our customers against unwanted and illegal robocalls. Indeed, our record of innovation confirms that we have been the industry leader at every stage of the fight against the robocalling scourge. Our customers have thoroughly embraced the various tools that T-Mobile offers to fight unwanted robocalls and scam calls.

T-Mobile first launched Scam ID and Scam Block—free, network-based scam detection tools—in March 2017, making T-Mobile the first voice service provider to deploy free scam protection at the network level. T-Mobile customers do not have to download an application or buy a particular device to get scam notifications; every postpaid T-Mobile customer and Metro by T-Mobile customer automatically gets Scam ID for free.

Scam ID labels highly probable incoming robocalls as "Scam Likely," and each customer can decide whether to answer those calls. Alternatively, customers who do not want to receive incoming calls labeled as "Scam Likely" may elect to engage our Scam Block tool for free by dialing #662# or activating the feature directly in their T-Mobile account.

To encourage customers to activate Scam Block and educate our customers on our cutting-edge blocking tools, T-Mobile held a virtual scam "Block Party" on July 15, 2019. To date, T-Mobile's efforts have allowed us to identify over 21 billion "scam likely" calls and block over five billion of those unwanted calls.

T-Mobile USA, Inc.
Office: 615-445-3800
695 Grassmere Park
Nashville, TN 37211

T-Mobile's network-based tools use artificial intelligence, machine learning, and call behavior as part of the reasonable analytics to examine the "fingerprint" of all incoming calls to detect and label likely scams. T-Mobile's network-based protections based on those analytics update ***every four to six minutes***, while application-based approaches are only as current as an application's last update. This constant analytical updating of incoming call fingerprints allows T-Mobile to keep up with scammers in almost real-time to protect our customers.

In addition to Scam ID and Scam Block, T-Mobile also offers a premium call control and caller ID service called "Name ID." Name ID allows a user to block individual numbers, "always allow" and "always block" specific numbers, and to perform reverse number lookup. In addition, it allows customers to choose the categories of robocalls they do or do not want to receive. With this application, customers can send the following categories of calls straight to voicemail — telemarketing calls, political calls, nuisance calls, survey calls and charity calls. Name ID is a subscription, application-based service, and the settings are saved at the network-level, so they transfer automatically to new devices and continue to work even when a device is turned off.

Name ID is included with Magenta Plus and T-Mobile ONE Plus plans and is available for $4/month per line for customers on other plans.

T-Mobile is also proud of its other important industry firsts:

- first to announce readiness for STIR/SHAKEN in 2018;
- first wireless provider to deploy STIR/SHAKEN standards on its network in January 2019, and;
- first wireless provider to implement cross-network STIR/SHAKEN authentication in April 2019.

Another outstanding achievement is that T-Mobile is capable of signing and authenticating 100% of SIP traffic that both originates and then terminates on our network. T-Mobile first authenticated calls on our own network in January 2019 when we launched a feature that displays the words "Caller Verified" on incoming calls that we can verify as authentic using STIR/SHAKEN. In April 2019, T-Mobile and Comcast Xfinity Voice Home launched cross-network robocalling protection built on STIR/SHAKEN standards, giving consumers confidence that calls from Comcast home phones to T-Mobile phones (and *vice versa*) are not generated by a scammer.

In August 2019, T-Mobile and AT&T Wireless began rollout of cross-network call authentication based on STIR/SHAKEN standards. In November 2019, T-Mobile, Comcast, and Inteliquent, Inc. announced an industry first in the war against spoofers and scammers after completing the first end-to-end STIR/SHAKEN call verification across three networks. Most recently, T-Mobile and Sprint announced their respective rollout of cross-network call authentication based on STIR/SHAKEN standards.

Device makers must implement software updates for customers to be able to see the "Caller Verified" display on calls, and today, STIR/SHAKEN is operable on 23 different T-Mobile and Metro by T-Mobile devices.

Finally, T-Mobile has been an active participant in key industry groups aimed at combatting unwanted robocalls—FCC Robocalling Strike Force, ATIS STI-GA Board, and USTelecom Traceback---for many years. T-Mobile's record demonstrates that it will continue leading the industry in protecting consumers from unwanted robocalls.