FCC Consumer Advisory Committee Recommendation Regarding Caller ID Authentication

While fraudulent caller ID spoofing—which is when a caller causes incorrect caller ID information to be displayed in order to commit fraud—has long been illegal,[1] it has become increasingly common in recent years. For example, consumers increasingly complain about "neighbor spoofing," in which the caller spoofs a number from the consumer's own area code and local exchange. According to the call-blocking service Nomorobo, while these calls constituted about 4 percent of unwanted robocalls in 2016, that number has shot up to 18 percent.[2]

Earlier this year, the Federal Communications Commission (FCC) released a Notice of Inquiry to learn more about the ways that it can facilitate the development of a technology, caller ID authentication, which can be a tool to help eliminate illegal caller ID spoofing[3] and unwanted calls. This inquiry is one of many efforts the FCC has been undertaking to address illegal and unwanted calls, and we commend the FCC's focus on these issues. Industry and consumer groups have recognized the promise of caller ID authentication. Because caller ID spoofing exacerbates the problems of illegal and unwanted robocalls—which remain the top complaint to the FCC[4]—we call on the FCC to encourage, as quickly as possible, the robust development of this technology that can help provide important consumer protections against these calls.

Caller ID spoofing can be utilized for legitimate reasons in some cases, (such as by domestic violence shelters to protect clients). However, caller ID spoofing can also pose threats to consumers. First, it can make consumers more vulnerable to phone scams when calls appear to be from trusted numbers or to be associated with trusted callers. If a trusted number appears in the caller ID, the called party is more likely to believe that the call is legitimate, and therefore may be more likely to part with their money or reveal financial and other personal information. Second, it is difficult to identify spoofed calls using existing call-blocking technologies as scammers modify their calling patterns, such as by unlawfully spoofing local numbers. Many current technologies make use of blacklists of numbers reported by consumers. In response, fraudulent callers commonly cycle through different spoofed numbers to evade blocks. For example, the call-blocking service Nomorobo updates its blacklist every hour in an effort to stay ahead of scammers.[5] Spoofed numbers reduce the utility of such lists.

Further, illegal caller ID spoofing poses challenges to law enforcement seeking to investigate and shut down fraudulent robocallers. While calls placed over traditional networks have numbers associated with a

[1] Fed. Commc'ns Comm'n, Spoofing and Caller ID, (last updated/reviewed Sept. 26, 2017), https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.
[2] Anthony Giorgianni, *The Newest Ways to Deal with Robocalls*, CONSUMER REPORTS (Nov. 13, 2017), https://www.consumerreports.org/robocalls/how-to-deal-with-robocalls/.
[3] In the Matter of Call Authentication Trust Anchor, Notice of Inquiry, WC Docket No. 17-97 (Rel. July 14, 2017), *available at* https://ecfsapi.fcc.gov/file/07141096201120/FCC-17-89A1.pdf. [hereinafter NOI].
[4] In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls, Notice of Proposed Rulemaking and Notice of Inquiry, CG Docket No. 17-59, Statement of Chairman Ajit Pai at 26 (Rel. March 23, 2017), *available at* https://ecfsapi.fcc.gov/file/0323136149698/FCC-17-24A1.pdf.
[5] Nomorobo, Background Updates (last visited Nov. 13, 2017), https://nomorobo.zendesk.com/hc/enus/articles/115001498406-Background-Updates.

physical location,[6] those placing calls over Internet Protocol can easily hide their identity using caller ID spoofing, making it more costly and time-consuming to ultimately identify the perpetrator—allowing them ample time to evade enforcement. As calls are typically routed through multiple carriers, it is even more time-consuming to investigate and trace calls to their origin. The use of caller ID authentication can make a positive contribution to speed the process of investigations and traceback.[7]

Caller ID authentication using the SHAKEN implementation of the STIR protocol presently is a promising solution to help address spoofing that leads to illegal or other unwanted robocalling. This technology allows for authenticating caller ID information and for that information to be transmitted to carriers along the call path. While several voice providers have already begun testing these protocols,[8] the technology is still currently in development. Once the technology is finalized and ready for implementation, the FCC should ensure that:

1. <u>All voice providers are encouraged to implement caller ID authentication as broadly and quickly as possible</u>. While the costs of adopting this technology may make it hard for some to implement, given the promise of this technology, the FCC should explore incentives to encourage widespread adoption.

2. <u>Service providers and third party call blocking services can offer consumers the ability to block, under appropriate circumstances, calls that fail to authenticate the caller ID information.</u> Consumers should have the option to block or decline potentially fraudulent calls as well as other unwanted calls. Such blocking may not yield perfect results but, with education, consumers can be empowered to use available and emerging tools.

3. <u>Consumers have better protections from spoofed calls originating internationally, which accounts for a significant portion of fraudulent calls</u>. The FCC notes in the NOI that "We anticipate that adopting authentication frameworks in the United States will naturally have less effect on foreign robocalling."[9] We urge the FCC to take steps to ensure that these systems protect consumers from illegal and unwanted robocalls originating internationally as they will from those originating domestically. This may require FCC action to encourage its counterparts in other countries to take a leadership role in promoting caller ID authentication, as failure by any part of the ecosystem to participate risks limiting the efficacy of efforts in the United States.

Additionally the FCC should:

[6] Henning Schulzrinne, "Telephone Numbers in an IP Environment," (presentation, IETF 92, Dallas, TX, March 26, 2015), approximately 23:30, http://recordings.conf.meetecho.com/Playout/watch.jsp?recording=IETF92_MODERN&chapter=chapter_0.

[7] Still Ringing off the Hook: An Update on Efforts to Combat Robocalls, Before the United States Senate Special Comm. on Aging, 115th Cong. 12-13 (2017) (testimony of the Federal Trade Commission), https://www.ftc.gov/system/files/documents/public_statements/1256863/p034412_commission_testimony_re_robocalls_senate_10-4-17.pdf.

[8] Jonjie Sena, It's Time to Hang Up on Robocalls for Good, Neustar Blog (May 16, 2017), https://www.neustar.biz/blog/hang-up-on-robocalls.

[9] *Id.* at ¶ 40.

1. Work collaboratively with industry and consumers groups to continue to explore tools and practices that effectively protect consumers from illegal and unwanted calls, including consumers with traditional landline service, who currently have fewer mitigation options than consumers with IP-enabled service.

2. Work with IP-based relay providers to ensure that all necessary steps are taken to make use of call authentication technology in their relay operations.

3. Continue its aggressive enforcement efforts that are targeting bad actors engaged in illegal robocalling activities. Where appropriate, the FCC should seek to partner with other federal law enforcement agencies to identify, target and bring to justice, including through criminal prosecution where warranted, bad actors engaged in illegal robocalling activities.

4. Encourage voice providers to make information available about the tools and options they provide to consumers to mitigate illegal and unwanted robocalls. This information should be easily available to current and potential subscribers.

5. Continue to study the tools and technologies being implemented by providers to protect consumers from illegal and other unwanted robocalls. This examination should include the various technology platforms used to deliver voice telecommunications services. Attention should also be paid to providers of all sizes and in different geographic service areas. Different providers may choose to implement different tools based on a variety of factors, such as technology limitations and cost.

Finally, we thank the FCC for its work on this issue. The FCC's efforts to explore how it can facilitate the development of caller ID authentication are important in the fight against robocalling abuse.

Adopted unanimously February 26, 2018
Abstentions: Americans for Tax reform

Respectfully submitted:
Eduard Bartholme, Chairperson
FCC Consumer Advisory Committee