Joan Marsh
Executive Vice President
Regulatory & State External Affairs

AT&T Services, Inc.
1120 20th Street NW
Suite 1000
Washington, DC 20036

T 202.457.3120
C 202 262 7479
jm3489@att.com

January 14, 2019

The Honorable Jessica Rosenworcel
Commissioner
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554

Dear Commissioner Rosenworcel:

On behalf of AT&T,[1] I write in response to your December 12, 2018 letter to John Donovan, CEO of AT&T Communications, inquiring about the consumer tools, and free tools in particular, that AT&T makes available to combat illegal and unwanted robocalls. As documented most recently in our comments in response to the public notice issued by the Consumer and Governmental Affairs Bureau,[2] AT&T offers a variety of such tools and, indeed, is an industry leader in the fight against the scourge of illegal and unwanted calls.[3] Consistent with that prior filing and others we have made in the proceeding referenced above, this letter provides a report on our efforts to-date, and identifies areas where we are continuing to work with the Commission to eliminate regulatory barriers currently preventing voice service providers from taking more aggressive steps against fraudsters.

---

1 AT&T Services, Inc. files this letter on behalf of AT&T Mobility and its wireline operating affiliates (collectively, "AT&T").

2 Public Notice, FCC, *Consumer and Governmental Affairs Bureau Seeks Input for Report on Robocalling*, CG Docket No. 17-59, DA 18-638 (rel. June 20, 2018).

3 Comments of AT&T, CG Docket No. 17-59 (filed July 20, 2018) ("AT&T Robocall Report Comments"); *see also* Comments of AT&T, CG Docket No. 17-59 (filed Sept. 24, 2018) (advocating for expanded provider-initiated call blocking authority) ("AT&T Robocall Record Refresh Comments").

A. AT&T Offers a Variety of Tools to Consumers To Combat Illegal and Unwanted Calls.

Recognizing that consumers need a whole toolbox of tools to stop robocalls,[4] AT&T offers multiple call blocking options across its platforms. Customers of AT&T's post-paid mobile wireless, interconnected VoIP, and legacy telephone services all have access to such options, many of which are available at no charge to the customer. While AT&T continues to innovate and improve in this area, below is a summary of AT&T's current offerings.

AT&T Call Protect. In December 2016, AT&T launched AT&T Call Protect for post-paid mobile wireless customers.[5] AT&T Call Protect is an opt-in service, available at no additional charge, that automatically blocks potential fraud calls and labels calls from telephone numbers identified with other suspect or potentially unwanted sources, including telemarketer, suspected spam, and other categories of calls. The service works across AT&T's nationwide wireless network, on any eligible iOS or Android smartphone,[6] whenever the subscriber is located in an AT&T HD Voice coverage area.[7] AT&T also offers the AT&T Call protect companion application (again, at no additional charge), which allows AT&T Call Protect subscribers to access additional features of the AT&T Call Protect service, including a personal block list.[8] While the app provides useful additional features, the AT&T Call Protect service does not require download or activation of the app. As of December 31, 2018, AT&T has blocked more than 391 million fraud calls, and labeled more than 552 million spam calls, through AT&T Call Protect.[9]

AT&T Call Protect Plus. AT&T Mobility customers with eligible iOS and Android devices also have the option to subscribe to AT&T Call Protect *Plus* for a charge of $3.99 per month.[10] AT&T Call Protect Plus offers all of the benefits of the free AT&T Call Protect service, plus a number of additional features, including enhanced caller ID and reverse number lookup.[11] AT&T

---

4 AT&T Blog Team, *We Need a Whole Toolbox To Stop Robocalls*, AT&T Global Public Policy Blog (Mar. 22, 2018, 11:36 AM), https://www.attpublicpolicy.com/consumers/we-need-a-whole-toolbox-to-stop-robocalls/.

5 *See* Press Release, AT&T, AT&T Unveils Call Protect To Help Customers Manage Unwanted Calls (Dec. 20, 2016), http://about.att.com/story/att_call_protect.html.

6 Phones must be HD Voice-enabled to be eligible. Eligible smartphones include iPhone 6 or above running iOS v9.3+ and AT&T HD Voice-enabled Android smartphone.

7 *See* https://www.att.com/esupport/article.html#!/wireless/KM1137805.

8 *See* https://www.att.com/esupport/article.html#!/wireless/KM1147710.

9 Call block totals for AT&T Call Protect are distinct from, and do not include, calls blocked through AT&T Call Protect Plus, Digital Phone Call Protect, and AT&T's other blocking programs, described herein.

10 *See* https://www.att.com/esupport/article.html#!/wireless/KM1252905. AT&T Call Protect Plus is offered together with the protection of the AT&T Mobile Security service.

11 *See id.*

Call Protect Plus users also have the option to identify entire categories of calls (e.g., political or survey calls) to block or send to voicemail (or accept) through the custom call control feature.[12]

Suspected Spam and Fraud Alerts. AT&T's most recent addition to the AT&T Call Protect suite of services launched just last month.[13] The new service, available on an opt-out basis for customers with eligible smartphones who enroll in one of our current post-paid wireless plans, is offered at no additional charge. The service labels calls from telephone numbers identified with suspect or potentially unwanted sources.

Digital Phone Call Protect. In November 2017, AT&T expanded AT&T Call Protect to customers of AT&T Home Phone,[14] AT&T's consumer VoIP service.[15] Much like AT&T Call Protect for mobile wireless customers, Digital Phone Call Protect is an opt-in service, offered at no additional charge to customers, that automatically blocks calls from known scammers, and sends customers a caller ID alert if a call is suspected spam.[16] As of December 31, 2018, AT&T has blocked more than 12.2 million incoming calls and labeled more than 11.7 million calls for Digital Phone Call Protect subscribers.[17]

AT&T Smart Call Blocker Phones. AT&T also has entered into a relationship with an equipment manufacturer and distributor to offer consumers an AT&T-branded telephone with call blocking capabilities. AT&T Smart Call Blocker phones work with any landline voice service (including legacy switched voice service) and on all wireline networks (not just AT&T's), for any consumer with caller ID.[18] AT&T Smart Call Blocker phones range in price from $59.95 to $119.95 and are manufactured by VTech. There is no additional charge for the call blocker features once the equipment is purchased. The phone screens incoming calls from telephone numbers not included on the consumer's list of trusted telephone numbers. Any such caller receives an intercept

---

12 *See id.*

13 *See* Barbara Roden, AT&T, *AT&T Extends Call Protection to More Customers Through Suspected Spam and Fraud Alerts* (Dec. 13, 2018), https://about.att.com/inside_connections_blog/2018/120/att_extends_call_protection.html.

14 In addition to the features of Digital Phone Call Protect, described herein, AT&T Home Phone customers may block up to 100 telephone numbers, simply by pressing *61 after receiving the unwanted incoming call. Customers also can set up and edit a call block list online through their myAT&T account.

15 *See* Press Release, AT&T, Protecting You From Unwanted Calls (Nov. 29, 2017), http://about.att.com/newsroom/unwanted_calls.html.

16 *See* https://www.att.com/esupport/article.html#!/u-verse-voice/KM1235421.

17 Call block totals for Digital Phone Call Protect are distinct from, and do not include, calls blocked through AT&T Call Protect, AT&T Call Protect Plus, and AT&T's other blocking programs, discussed herein.

18 *See* https://telephones.att.com/telephones/cordless-telephones/smart-call-blocker.

message and is required either to press a key or to record his/her name before the call will ring through to the consumer. This intermediate step, among other benefits, has the effect of diverting callers who are not live persons. Such a screen therefore helps to eliminate certain illegal and unwanted robocalls that use an artificial or pre-recorded voice.

Consumer Information and Education. While consumer call blocking tools are an integral part of AT&T's fight against illegal and unwanted robocalls, educating consumers about known threats and common fraudster tactics also are critically important. AT&T's Cyber Aware Resources page includes alerts on recently identified scams and provides links to other important consumer resources, as well as instructions for reporting various types of fraud (including telephone call fraud).[19] AT&T pushes this educational content through social media and digital advertising. AT&T also issues consumer alerts when fraud events are identified.[20]

B. AT&T Is Blocking Illegal Traffic on Its Network Where Legally Permitted.

Separate and apart from the consumer tools that AT&T offers, AT&T has developed and deployed other network-based call blocking capabilities to combat the volume of illegal traffic directed at consumers. Indeed, as is now well-documented, AT&T launched a program in late 2016 to identify and block illegal traffic delivered to AT&T from providers purchasing AT&T's IP-based call termination service. Consistent with the terms of the contractual arrangements with customers of its IP-based call termination service, AT&T blocks calls from telephone numbers that it determines constitute prohibited traffic on its network.[21] Since its inception, the program has prevented approximately 4.5 billion illegal calls from ever reaching their intended destination. AT&T has designed its call blocking program to target only illegal robocalls and has developed and implemented robust detection and investigative techniques. Leveraging big data intelligence, AT&T monitors its network for suspicious traffic. When identified, AT&T's team of experienced fraud investigators opens an investigation. Their investigation involves multiple steps, often including: gathering additional call detail information, online research, and outreach to service providers to authenticate the fraud team's independent investigation. Critically, among other steps AT&T takes to avoid impacting legitimate traffic, every suspect telephone number is dialed by a fraud investigator

---

19 *See* http://about.att.com/sites/cybersecurity/resources/contact. *See also, e.g.*, https://www.att.com/robocalls; https://about.att.com/sites/cyberaware/ni/blog/caller-id-spoofing; https://about.att.com/sites/cyberaware/ae/robocall; https://www.att.com/esupport/report-call-or-text.html.

20 *See, e.g.*, http://about.att.com/sites/cybersecurity/ar/wangiri; https://about.att.com/sites/cyberaware/ar/lottery_scam; https://about.att.com/sites/cyberaware/ar/irs_scam.

21 *See* Letter from Vonda Long-Dillard, AT&T, to Marlene H. Dortch, FCC, CG Docket No. 17-59, at 1 (filed Sept. 22, 2017).

before a block is placed. Once the investigator is reasonably confident that a telephone number is engaged in the transmission of Prohibited Traffic (as that term is defined in the AT&T Business Service Guide), a block is put on the telephone number. The fraud team continues to review the activity so that the block can be removed once the illegal activity has ceased. While AT&T invested considerable time and expense to develop and operationalize the program, consumers receive the benefit of this call blocking program at no charge.

Additionally, AT&T was among the first to implement the *2017 Call Blocking Order* when it took effect.[22] Since that time, AT&T has prevented approximately 19.8 million illegal calls from reaching its post-paid wireless customer base, including fixed and mobile wireless customers.[23]

As we have explained in previous submissions, AT&T stands ready, willing, and able to target and block illegal traffic more aggressively on its network. Indeed, AT&T is eager to expand its call blocking programs for the benefit of our customers. As we have detailed in previous filings in this proceeding, the Commission should authorize broader provider-initiated call blocking consistent with the best practices developed and implemented by AT&T's fraud experts in our call blocking programs, and the Commission also should propose and adopt a safe harbor to insulate voice service providers that engage in call blocking from liability in the event the provider inadvertently blocks a legitimate call.[24] AT&T has proposed a framework for such a safe harbor. We would welcome your support of these proposals.

C. AT&T Is, and Will Continue To Be, a Leader in the Fight Against Illegal and Unwanted Robocalls.

Significantly, AT&T's efforts are not limited to call blocking and labeling. Far from it. We are actively engaged with industry stakeholders on a number of additional fronts in the fight against illegal and unwanted robocalls, as further described below.

SHAKEN/STIR. As detailed in our recent response to Chairman Pai on the implementation of caller ID authentication technology,[25] AT&T has played a leading role in the

---

[22] *See* AT&T Robocall Report Comments at 9.

[23] Call block totals identified in connection with the *2017 Call Blocking Order* are distinct from, and do not include, calls blocked through AT&T Call Protect, AT&T Call Protect Plus, Digital Phone Call Protect, and AT&T's other blocking programs, discussed herein.

[24] *See generally* AT&T Robocall Record Refresh Comments; AT&T Robocall Report Comments at 9-14.

[25] *See* Letter from Joan Marsh, AT&T, to Chairman Ajit Pai, CG Docket No. 17-97 (filed Nov. 19, 2018).

development of the technical protocols known as Signature-based Handling of Asserted Information Using toKENs and the Secure Telephone Identity Revisited ("SHAKEN/STIR"). That leadership continues today as industry enters the implementation phase of SHAKEN/STIR. AT&T will be among the first in the industry with the ability to sign calls and exchange certificates with other providers. In addition, AT&T's representative chairs the Secure Telephone Identity Governance Authority board, which is presently establishing the policy framework for the operation of SHAKEN/STIR.

Industry Traceback Process. AT&T also is proud to have worked cooperatively with industry partners to develop and implement the industry traceback process, overseen by USTelecom, which maps a call's path through multiple networks to identify the call originator. Traceback has been an important investigative tool for law enforcement, giving investigators information they need to identify and shut down illegal robocall and scam operations, including operations located overseas. AT&T and its industry partners meet twice a month (and more frequently, as needed) to discuss current issues and solutions, including potential process and efficiency improvements to the traceback process. Participating service providers also routinely initiate numerous tracebacks themselves in an effort to build cases against bad actors perpetrating fraud among consumers that they can then share with law enforcement authorities at the Commission, FTC, FBI, and others.[26]

Engagement with Call Originators. Looking beyond the cooperative efforts of voice service providers to combat illegal and unwanted calls, AT&T has established an ongoing and constructive dialogue with call originators to understand and, where appropriate, address concerns they have raised. AT&T is not unsympathetic to the complaints of legitimate, law abiding call originators, who have seen call answer rates decline as consumers increasingly use call blocking/labeling tools and/or simply no long answer calls from unfamiliar telephone numbers. AT&T is committed to accuracy and will make improvements to its consumer tools where appropriate and feasible.[27]

---

[26] AT&T would welcome—and, in fact desires—more vigorous enforcement activity. In AT&T's view, developing cases at the industry level, coupled with enforcement action, may be the most productive way to reduce illegal robocalls at the source, as tracebacks often point to a limited number of bad actors as the perpetrators of a large number of illegal robocalls. Enhancing law enforcement resources thus has the potential to have the greatest impact in addressing the illegal robocall problem.

[27] At the same time, AT&T fully embraces the reality that services like AT&T Call Protect, among others, provide consumers with useful information about the calls they receive, and that many consumers simply do not want to take calls from businesses or telemarketers—even those with which the consumer has (or had) a relationship. Consumers who have subscribed to a service within the AT&T Call Protect suite value the information those

* * * * *

AT&T appreciates the Commission's continued attention to the scourge of illegal and unwanted calls, including this opportunity to provide an update on our efforts to provide consumers with no- and low-cost tools to combat such calls. But our work is far from complete. AT&T thus remains steadfast in its commitment to working to find new, and improve upon existing, methods of addressing this serious issue. As outlined above and detailed in our previous submissions in this proceeding, we encourage the Commission to provide voice service providers with greater flexibility to continue to attack the problem, and we look forward to working with you toward that goal.

Respectfully submitted,

/s/ Joan Marsh

Joan Marsh
Chief Regulatory & State External Affairs Officer
AT&T Communications

cc (via email): The Honorable Ajit Pai
The Honorable Michael O'Rielly
The Honorable Brendan Carr

services provide, in many cases because such services enable them to avoid calls from businesses and telemarketers.

David Morken
CEO and Co-Founder
900 Main Campus Drive
Venture III
Raleigh, NC 27606

January 14, 2019

Sent Via Email

Honorable Jessica Rosenworcel
Commissioner
Federal Communications Commission
445 12th Street, SW Room TW-A325
Washington, DC 20554

Dear Commissioner Rosenworcel:

Pursuant to your letter of December 12, 2018, I am writing on behalf of Bandwidth Inc. ("Bandwidth") regarding Bandwidth's efforts to adopt systems, processes and procedures to help protect its customers and the broader communications industry ecosystem from the harms of illegal robocalling fraud and abuse. Bandwidth operates a network that is entirely optimized for Internet Protocol ("IP") technology and predominately acts in the capacity of an underlying service provider to other innovative IP-based communications service providers. As a result, Bandwidth is not typically positioned to offer consumer-oriented tools directly to end users itself, but is rather working to structure its underlying services in a manner that allow its customers to deploy the kind of consumer-oriented solutions your letter appears to contemplate.

To that end, Bandwidth is actively engaged in efforts to implement the most robust call authentication framework possible, while also working diligently to stop the transmission of illegal robocalling on its network holistically. Bandwidth has adopted a three-pronged operational approach (prevent, detect, and mitigate) to stopping illegal robocalls in keeping with the industry efforts and best practices. Bandwidth's three-pronged operational procedures are summarized as follows:

- *Prevention:* Bandwidth has launched a series of customer communications aimed to clarify what constitute unlawful robocalls and instructs our customers to take all necessary steps to prevent these types of calls from originating from their networks. Bandwidth has implemented a stringent screening process designed to prevent potential robocalling companies from becoming Bandwidth customers.

- *Detection:* Bandwidth has implemented processes and procedures to detect and analyze campaigns on our network to determine if they are lawful or not. When unlawful robocall campaigns are detected, Bandwidth works to stop the unlawful activity as quickly as possible. Bandwidth is also in the midst of augmenting it's robocall detection technologies which are expected to dramatically improve our ability to rapidly detect and react to suspected robocall behaviors.

- *Mitigation:* Bandwidth has also developed call blocking tools that prevent calls with specific unlawful telephone number characteristics from traversing the Bandwidth network. Bandwidth personnel regularly analyze network traffic for unlawful robocall campaigns and utilize our call blocking tools when appropriate. Bandwidth also initiates trouble tickets with customers that we've identified to be in the path of unlawful robocalls. Then we work diligently together with our customers to stop the unlawful robocall campaigns detected.

In addition to incorporating these operational procedures into its services on behalf of its customers, Bandwidth also manages and operates a SPAM messaging filter tool in the core of network. Its ability to identify and prevent the delivery of unwanted messaging traffic in the core of its network is a benefit to consumers that Bandwidth does not charge for additionally. Further, Bandwidth is an active participant and leader in industry organizations and industry efforts to stop illegal robocalling. Even prior to the establishment of the Robocall Strike Force,[1] Bandwidth was engaging the FCC and the FBI in efforts to stop consumer fraud in the form of Toll Free Traffic pumping, and participating in the USTA sponsored traceback efforts to identify robocall originators and support enforcement. Bandwidth works closely with the FCC, FTC, FBI and IRS among others in law enforcement and is actively engaged in working groups and at the board of director level at SIPForum, CTIA, Incompas, and SOMOS in their respective efforts to address the consumer threats of robocalling. Bandwidth is also a member of the NANC, served on the NANC's CATA Working Group and has been selected to be the Incompas representative on the ATIS STI-GA Board in charge of overseeing the procurement of vendors for the critical components of the SHAKEN/STIR framework such as the Certificate Authority and the Policy Administrator. Finally, Bandwidth is also a paid member and participant in the Communications Fraud Control Association (CFCA).

---

[1] *See:* FCC to Host First Meeting of Industry-Led Robocall Strike Force, Public Notice, DA 16-917 (rel. Aug. 12, 2016).

Thank you for your attention to the importance of protecting consumers in today's environment. Bandwidth looks forward to continuing its work to simultaneously advance the consumer benefits of competition and innovation in the communications marketplace while protecting consumers from the dangers of illegal robocalling. Should you have any additional questions or concerns, please do not hesitate to contact us.

Sincerely,

David Morken

Cc: Ms. Jessica Martinez

David C. Bartlett
Vice President
Federal Government Affairs
1099 New York Ave., NW, Suite 250
Washington, DC 20001
202-429-3101

January 14, 2019

Hon. Jessica Rosenworcel
Commissioner
Federal Communications Commission
445 Twelfth Street, SW
Washington, DC 20554
jessica.rosenworcel@fcc.gov

Dear Commissioner Rosenworcel:

I am pleased to answer your December 12 letter about CenturyLink's tools to help consumers reduce annoying and unlawful calls. We share your concern about illegal robocalling and the frauds and scams commonly associated with it.

Low-cost Internet based calling platforms have led to large scale robocalling campaigns, worsened by increasingly sophisticated Caller ID spoofing that makes calls appear more credible and that make it difficult to pursue or block fraudsters. Perhaps the worst robocalling offenders are overseas, in markets not noted for respecting consumers or U.S. laws.

Unwanted calls annoy us all. They harm consumers and diminish trust in voice service. That is why CenturyLink has been working with industry and trade associations on new industry technology to reduce the problem through a variety of means. New call authentication technology promises to help industry reduce illegal robocalls, increase confidence in Caller ID, and make it easier to identify suspect calls and trace back illegal ones. Where technically feasible, SHAKEN/STIR is being rolled out broadly by the industry in 2019, including CenturyLink. In the meantime, existing consumer tools can help reduce unwanted calls.

CenturyLink offers a variety of tools to help our customers control who can reach them. Even with growth in spoofing, *Caller ID* can help consumers recognize and decline to answer suspicious calls. *Caller ID with Privacy+* blocks calls that lack Caller ID information unless the caller provides a name. *Anonymous Call Rejection* blocks calls from "private" or anonymous numbers. *Call Rejection* and *Enhanced Call Rejection* block calls from specific numbers. *Do*

Not Disturb and *Call Curfew* block all incoming calls during specified hours. CenturyLink also offers a *Call Trace* service for harassing or disturbing calls.

Our call screening tools are even more effective against robocallers. CenturyLink's innovative *No Solicitation* services plays an automated message asking solicitors to hang up and telling legitimate callers to press a specific key. Otherwise, the call never rings through to the customer and instead is forwarded to voice mail. CenturyLink's *Security Screen* requires callers from blocked, unidentified, toll-free or long distance numbers to enter their ten digit telephone numbers before their call will connect to the customer. Although *No Solicitation* and *Security Screen* services do not actually block robocalls, our experience shows they dramatically reduce unwanted calls by frustrating automated platforms and discouraging live robocalling operators. These call screening tools are among our most popular features, which reflects their high level of practical effectiveness.

These calling features-are available today at no additional cost with most home or business phone bundles. For basic phone customers without bundled service – who represent a small fraction of voice accounts – a modest monthly fee applies, with pricing varying by location. Availability also varies by state and by local operating company based on local network. I am enclosing a list of current tools and their typical cost.

CenturyLink is also evaluating new features that will make use of Call Authentication signaling enabled by the 2019 rollout of the new SHAKEN/STIR technology. For Internet Protocol and TDM network, CenturyLink engineers are evaluating options to enhance our customer tools, notably by supplementing Caller ID displays based on Call Authentication., This should provide consumers with greater confidence in the calls they may receive. Although there are challenges with authentication for calls involving networks based on Time Division Multiplexing, there are potential solutions that may enable many IP-originated inbound calls to be recognized as authenticated.

We are also looking at new uses of data analytics in conjunction with SHAKEN/STIR for new network blocking and consumer blocking and screening options. Vendors are rapidly developing new products and services, and CenturyLink is evaluating new tools to add to its network with the 2019 rollout of the new technology. Additionally, SHAKEN/STIR will enable CenturyLink and allied providers to enhance the speed and effectiveness of their Trace Back initiative, which works to identify originators of unlawful robocalls.

CenturyLink is doing its part to help address the difficult problem of illegal robocalls. Our consumer tools can help, and we encourage customers to use them to help reduce unwanted calls.

Sincerely,

encl.

BLOCKING & SCREENING TOOLS

CenturyLink's website provides tips on how to reduce unwanted calls, as well as detailed information about tools that can be used to block or filter calls. The website describes each feature, how it can be used, and how it can be effective. Availability of particular calling features varies depending on local network. Additional tools are under review based on new Caller ID authentication technology being deployed across the industry in 2019.

Ways to block unwanted calls from your home phone.
http://www.centurylink.com/help/help/index.php?assetid=183

How to use calling features to block incoming calls.
http://www.centurylink.com/help/?assetid=233

Caller ID

Caller ID helps customers recognize unfamiliar callers that they may not want to answer. Consumers utilize Caller ID routinely to screen inbound calls and avoid suspected robocallers.
The service is included for customers with a Home Phone or Small Business bundle at no additional cost. For Basic Phone customers with local service, a monthly fee of $6 to $10 applies.

Security Screen

Security Screen blocks calls from blocked, unidentified, toll-free, or long distance calls unless the caller provides a number. This feature is highly effective at frustrating most robocallers and avoiding the annoyance of answering.
This feature is included for customers with a Home Phone or Small Business bundle at no additional cost. For Basic Phone customers with local service, there is a $2.95 monthly fee.

Caller ID with Privacy+

Caller ID with Privacy+ blocks calls that lack Caller ID information, unless the caller provides a name.
The customer can hear the name and decide to accept or decline the call. The screening step can frustrate many automated robocalling platforms and reduce the annoyance of answering unwanted calls.
This optional service is available to all customers at a $2.95 monthly fee.

Call Rejection/Enhanced Call Rejection

Call Rejection blocks up to 15 unwanted numbers selected by the customer. This feature can help block repeats of unwanted calls, although it is not effective against robocallers that falsify and repeatedly change their Caller ID.
It is included for customers with a Home Phone or Small Business bundle at no additional cost. For Basic Phone customers with local service, there is a $6 monthly fee.

Enhanced Call Rejection blocks up to 25 unwanted numbers.
It is included for customers with a Home Phone or Small Business bundle. For Basic Phone customers with local service, it is $6 per month.

Anonymous Call Rejection

Anonymous Call Rejection blocks calls that lack Caller ID information, such as “private” numbers. It is effective against robocallers that block their originating number, but not against those that falsify their originating number.
It is included for customers with a Home Phone or small business bundle at no additional cost. For Basic Phone customers with local service, it is offered at no additional charge with *Caller ID* service.

No Solicitation

No Solicitation intercepts and plays a recording to callers, directing telemarketers to hang up.
Other callers may press "1" to have the call connected. This feature is highly effective at frustrating most robocallers.
This feature is included for customers with a Home Phone or Small Business bundle at no additional cost. For Basic Phone customers with local service, there is a $6.95 monthly fee.

Do Not Disturb/Call Curfew

Do Not Disturb stops all incoming calls when activated. *Call Curfew* stops all calls (incoming and outgoing) during periods the customer chooses. These tools can prevent the annoyance of unwanted calls at specific times, although they do not specifically target robocalls.
These features are included for customers with a Home Phone or Small business bundle at no additional cost. For Basic Phone customers with local service, there is a $3.95 monthly fee.

Call Trace

Call Trace allows consumers to report harassing or disturbing calls. After three traces, CenturyLink will take further action on request.
For all customers, there is a charge of up to $5 per use. There is no charge for unsuccessful traces.

* * *

Notes:

Charges vary by state and local operating company and may be somewhat lower in some locations. For Basic Phone customers, a one-time set-up fee may apply, which will vary by state and local operating company. Feature availability varies by local operating company.

Caller ID service and related features may be unavailable for technical reasons in a very small number of CenturyLink exchanges.

Charter
COMMUNICATIONS

Thomas M. Rutledge
Chairman and Chief Executive Officer

January 14, 2019

The Honorable Jessica Rosenworcel
Commissioner
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554
Jessica.Rosenworcel@fcc.gov

Dear Commissioner Rosenworcel:

Thank you for your letter asking what tools we offer our customers to combat robocalls. Charter is committed to combating the scourge of illegal robocalls and we appreciate you and the FCC taking action and making this important consumer protection issue a priority.

Charter has a long history of empowering and protecting consumers against bad actors. As we've noted before, we are working collaboratively with other stakeholders to implement the Signature-based Handling of Asserted Information using toKENs protocols and procedures, leveraging the Secure Telephone Identity Revisited protocol (together the "SHAKEN/STIR" Framework), throughout our footprint. We also support the adoption of rules that would permit providers to block calls that fail authentication where both the originating and terminating provider have implemented the SHAKEN/STIR Framework.

In addition to these industry-wide efforts, we are taking a number of measures now to protect our customers. We provide several call blocking and screening solutions for Spectrum Voice® residential customers, all of which are provided for free to our subscribers:

- *Accept Selected Callers:* Spectrum Voice customers have the ability to receive calls only from numbers they specify. Callers from phone numbers not contained on a pre-approved list will hear a polite message stating that calls are not being accepted at this time.

- *Block Anonymous Calls:* Spectrum Voice subscribers have the ability to block incoming calls that are presented without Caller ID information. Anonymous callers will hear a message stating that anonymous and private calls are not being accepted and instructing the caller to enable Caller ID before calling again.

- *Block Unwanted Callers:* A Spectrum Voice subscriber may create a list of numbers that will be blocked from ringing through to the user; such callers will hear a message stating that the customer is not accepting calls.

- *Caller ID:* Caller ID displays the incoming caller's phone number and name (if available), allowing the customer to screen for known numbers.

- *Call Waiting with Caller ID:* This feature identifies incoming calls when a subscriber is already on the phone. The subscriber can view the caller's information and determine whether or not to answer the call.

Charter also participated on the Robocall Strike Force and agrees with its conclusion that consumer choice is critical to effectively managing illegal robocalls. We are proud to have been an early mover on empowering consumers with Nomorobo, a third-party application to control unwanted inbound voice traffic, like telemarketers and robocallers. We partnered with Nomorobo in 2016 to provide free access to Spectrum Voice customers. In 2017, following significant investment, we made Nomorobo available across our footprint with a simplified "1-click" solution that can be activated via Charter's customer-facing voice feature management portals. As a result, hundreds of thousands of our customers have signed up for Nomorobo.

By using "Simultaneous Ring" functionality, Nomorobo receives calls at the same time as the subscriber. Nomorobo then instantaneously screens each call using a database of blacklisted phone numbers, including those on the "Do Not Call Registry," as well as an extensive "whitelist" of emergency services, such as hospitals and schools, to avoid false positives. If a call is flagged by Nomorobo for potential blocking, the caller receives a message asking for a 2-digit key: If the caller enters the two digits, the call is directed to the customer; otherwise, the caller is instructed that the answer was incorrect, and the call is not connected.

With respect to our enterprise customers, Charter offers a Custom Caller ID feature, which enables a customer to define the telephone number that appears to call recipients using Caller ID. Our terms of service require that the telephone number chosen must be active and assigned to the enterprise customer. We also require that the customer ensure 911 and other emergency calls are routed to an appropriate public safety answering point or other responding agency, based on the caller's location, in a manner consistent with applicable law. Telemarketers using this feature agree to comply with federal and state law, including obligations requiring identification of the telemarketer or the party on whose behalf the telemarketing call is being made and the calling party's number, automatic number identification, or the customer service number of the party on whose behalf the telemarketing call is being made. The use of substitute or fictitious information is prohibited.

Charter views combatting robocalls as a priority, and we stand ready to support the Commission as it continues to work on tackling illegal robocalls.

Sincerely,

Thomas M. Rutledge

400 Atlantic Street - 10th Floor | Stamford, CT 06901 | 203-905-7999

COMCAST

January 14, 2019

Commissioner Jessica Rosenworcel
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Dear Commissioner Rosenworcel:

On behalf of Comcast Corporation, thank you for your letter of December 12 to our Chairman and Chief Executive Officer, Brian Roberts, regarding our continued efforts in coordination with the Commission to address the scourge of illegal robocalls. As Senior Vice President and General Manager, Broadband, Automation and Communications at Comcast Cable, I have played a lead role in ensuring that tools mitigating these abusive calling practices are available to Comcast's customers, and Mr. Roberts thus has asked me to provide this response to your letter.

Comcast deeply appreciates the critical role the Commission has played—and is continuing to play—in giving voice providers the flexibility to deploy robocall mitigation tools for the benefit of consumers. In 2015, the Commission issued a ruling clarifying that voice providers may make call-blocking technology available to their customers who choose to use such technology to stop unwanted robocalls. Then, in 2017, the Commission adopted its *Robocall Blocking Order*, specifically permitting voice providers to block calls appearing to originate from invalid, unallocated, and unassigned numbers, as well as from numbers on the industry Do-Not-Originate (DNO) list. The Commission also has been active in promoting the development and implementation of the end-to-end call authentication protocol known as SHAKEN (Signature-based Handling of Asserted Information Using toKENs) and STIR (Secure Telephone Identity Revisited)—an initiative that Comcast has led on the industry side.[1] Separate from but in parallel with these efforts, the Commission's recent *Reassigned Numbers Order*, which set in motion the creation of a comprehensive database of number reassignments, provides yet another vehicle for reducing unwanted communications by enabling legitimate businesses to minimize inadvertent calls to wrong numbers.

---

[1] As noted in the letter of Comcast's Tony Werner to Chairman Pai on November 19, 2018, Comcast's Chris Wendt co-chairs the work group of the Alliance for Telecommunications Industry Solutions on the SHAKEN framework for caller ID authentication, is a primary author of the STIR specifications adopted by the Internet Engineering Task Force, and leads the development team pioneering an open source implementation of the specifications to promote testbeds and interoperability lab trials in the industry. Mr. Wendt also co-chaired the Authentication Work Group of the Robocall Strike Force, which was organized in 2016 to accelerate the development and adoption of new tools for mitigating fraudulent robocalls and has provided two detailed reports on those efforts to the Commission. Moreover, Comcast's Beth Choroser co-chaired the North American Numbering Council's Call Authentication Trust Anchor Working Group, which in May 2018 prepared a report for the Commission on the governance framework and timely deployment of the SHAKEN/STIR protocol.

Building off the Commission's multi-pronged efforts in this arena, and recognizing that consumers desire immediate relief from unwanted calls, we at Comcast seek to empower our customers with a variety of free tools and functionalities to mitigate robocalls. We currently offer free Nomorobo compatibility to all of our residential Xfinity Voice customers with Unlimited or Unlimited Select plans—representing 93 percent of our active residential voice customer base.[2] Nomorobo is a third-party cloud-based service that can be configured by consumers to block various types of robocalls, and was featured at the Commission's expo on robocall mitigation technologies in April 2018. We provide an easily accessible webpage instructing customers on how to activate the service,[3] and we are continuing to see a steady rise in the number of customers who take advantage of this offering. We estimate that this service successfully blocks roughly 10 million unwanted robocalls bound for Comcast customers every month.

We also have begun implementing free tools at the network level that employ specific robocall mitigation techniques authorized by the Commission's 2017 *Robocall Blocking Order*. For our residential Xfinity Voice customers, we have configured edge devices on our voice network to implement blocking of calls from numbers on the industry DNO list, and we block thousands of fraudulent robocalls through this method each month. Also, in the near future, we plan to begin deployment of a centralized capability for blocking calls appearing to originate from certain invalid and unallocated numbers and bound for residential Xfinity Voice customers. By implementing such call blocking in a centralized fashion, we not only can block a significantly greater volume of fraudulent robocalls, but also can move swiftly to add or remove numbers or ranges of numbers to be blocked as the need arises. In conjunction with these efforts, Comcast is an active member of the Industry Traceback Group, a coordinated initiative to trace abusive calls to their source and to identify callers likely to be engaging in fraudulent activity.

Moreover, as described in greater detail in the letter from Comcast's Tony Werner to Chairman Pai on November 19, 2018, we are pursuing an aggressive timeline for implementing an end-to-end call authentication capability based on the SHAKEN/STIR protocol for our residential Xfinity Voice subscribers—another robocall mitigation tool that will come at no additional cost to our customers. Indeed, in addition to being at the forefront of developing the SHAKEN/STIR protocol, we are leading the way in deploying this technology. I am pleased to report that we have now implemented the capability to sign calls originating from our residential Xfinity Voice customers for our entire residential subscriber base. Moreover, by the end of March 2019, absent any unexpected difficulties, we expect to have implemented the capability to verify calls that contain a SHAKEN/STIR-compliant signature for our entire residential subscriber base. Accordingly, by that time, all calls originating from a Comcast residential subscriber and terminating with a Comcast residential subscriber will be able to be signed and

---

[2] For the small portion of our residential voice customers who subscribe to legacy plans that lack compatibility with Nomorobo's technology, we are actively exploring solutions to bring the benefits of Nomorobo to those customers.

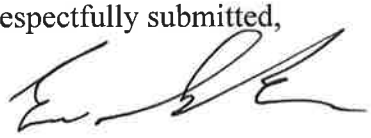
[3] *See* Comcast, "How to Stop Unsolicited Robocalls to Your Home," https://www.xfinity.com/support/articles/nomorobo.

verified in accordance with the SHAKEN/STIR framework. Comcast's implementation of signing and verification capabilities by that time also will enable the company to begin interoperating with other voice providers that have implemented such capabilities—thus paving the way for industry-wide call authentication that will thwart illegal spoofers of caller ID information.

In addition to these tools for Comcast's Xfinity Voice residential customers,[4] Comcast is actively raising awareness about available tools for Xfinity Mobile subscribers. Comcast maintains an easily accessible website providing Xfinity Mobile subscribers with lists of robocall mitigation apps available for iPhone and Android devices, and a large number of those apps are free to consumers.[5] As for network-level blocking functionalities, Xfinity Mobile's status as a mobile virtual network operator (MVNO) offering provided over Verizon's cellular network means that it is reliant on Verizon's own implementation of such tools, and Comcast will continue to work closely with Verizon to ensure that Xfinity Mobile customers receive the same robocall protections as Verizon Wireless retail customers.

As reflected in the efforts described above, Comcast is fully committed to empowering its customers with tools to combat the rising tide of illegal robocalls. We very much appreciate your inquiry into these issues and look forward to continuing our close work with the Commission in putting an end to these abusive practices once and for all.

Respectfully submitted,



Eric Schaefer
Senior Vice President and General Manager,
Broadband, Automation and Communications,
Comcast Cable

cc: Brian Roberts, Chairman and CEO, Comcast Corporation

---

[4] On the wireline side, because nearly all of the complaints Comcast receives regarding illegal spoofed robocalls are from our residential subscribers, we have prioritized implementation of robocall blocking tools for those subscribers. Comcast hopes to begin implementation of SHAKEN/STIR functionality for small business customers by the end of 2019 or the first half of 2020, followed by implementation for enterprise customers thereafter, and is actively exploring other robocall mitigation tools for these customers.

[5] *See* Comcast, "How Do I Block Robocalls," https://www.xfinity.com/mobile/support/article/360000902823/how-do-i-block-robocalls.

Jennifer Hightower
Senior Vice President and General Counsel

Cox Communications – Law & Policy
6205-B Peachtree-Dunwoody Road
Atlanta, GA 30328
404 269-7364
Jennifer.Hightower@cox.com

January 15, 2019

Commissioner Jessica Rosenworcel
Federal Communications Commission
445 12th St., S.W.
Washington, DC 20554

Re: *Call Authentication Trust Anchor*, WC Docket 17-97
Advanced Methods to Target and Eliminate Unlawful Robocalls, CG Docket 17-59

Dear Commissioner Rosenworcel:

In response to your letter to Pat Esser, president of Cox Communications, Inc., dated December 12, 2018, Cox is pleased to provide the following information.

Cox agrees that fraudulent and unwanted robocalls are a growing nuisance for consumers, businesses and service providers. Cox is committed to a comprehensive long-term industry solution and is making free tools available to its customers as it rolls out its next generation network to address the problem in the short-term.

Cox has been working with others in the industry and the FCC to develop a long-term solution that can adapt to the changing tactics deployed by bad actors. Cox detailed its participation and implementation plan for the SHAKEN/STIR framework in its response, dated November 19, 2018, to FCC Chairman Ajit Pai's letter from November 5, 2018.[1]

Cox is committed to implementing a robust call authentication framework in 2019. Cox has been actively involved for several years in the efforts to develop the SHAKEN/STIR framework in various industry standards fora. This includes participation on The Alliance for Telecommunications Industry Solutions (ATIS)/SIP- Forum IP-NNI Task Force and the Robocall Strike Force. Cox was also a participant in the Call Authentication Trust Anchor (CATA) working

[1] Letter from Jennifer Hightower, Cox Communications, to Chairman Ajit Pai, FCC, WC Docket 17-97 (filed November 19, 2018).

group of the North American Numbering Council (NANC). And today, Cox is engaged in the ATIS activities involving the establishment of the SHAKEN/STIR governance authority.

In the meantime, as industry continues its work on and deployment of SHAKEN/STIR and as Cox continues its current transition of its residential customer base to a new IP Multimedia Subsystem (IMS) platform, Cox is rolling out free access to Nomorobo. This third-party cloud-based service, which was featured at the FCC's expo on robocall mitigation techniques in April 2018, automatically intercepts and hangs up on robocallers and telemarketers. The Nomorobo service should be available to the vast majority of Cox's residential customers on the new voice services platform throughout 2019.

In addition, on behalf of its customers, Cox currently participates in two programs that were developed as part of the FCC's Robocall Strike Force effort. The first is the "Do Not Originate" activity that blocks calls where the originating telephone number is explicitly prohibited from originating calls, such as calls spoofing the IRS's customer care telephone numbers. The second is the "Traceback" activity that allows a customer to file a complaint with their service provider about a call they have received; their service provider can contact the originating carrier (if known) and have the originating carrier investigate and potentially shutdown the bad actors.

Cox is supportive of the Commission's efforts to stop unwanted robocalls and will do its part to ensure the success of those efforts.

Sincerely,

Jennifer Hightower
Senior Vice President and General Counsel
Cox Communications

Daniel McCarthy
President and CEO
401 Merritt 7
Norwalk, CT 06851

January 14, 2019

VIA EMAIL

Commissioner Jessica Rosenworcel
Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

Dear Commissioner Rosenworcel,

Thank you for your December 12, 2018 letter asking about the tools that Frontier offers to combat robocalls. Frontier applauds the Commission's continued leadership on reducing robocalls and supports the Commission's objective of making tools available to consumers to help fight the problem. Frontier makes several free tools available to assist consumers in stopping these unwanted calls and continues to work towards additional solutions to combat the bad actors that create this nuisance.

As the Commission is aware, technological capabilities play an essential role in our ability to stop robocalls. For customers who subscribe to a VoIP service, Frontier has promoted the award-winning "Nomorobo" service as a free solution to allow customers to effectively limit robocalls. We provide our customers with directions on how to enable Nomorobo for their Frontier service on our website, and VoIP customers have found the service to be a valuable tool in reducing unwanted robocalls.

Many of our phone customers also subscribe to traditional TDM voice service; although there are many benefits to a TDM-based voice call, it is more technologically challenging to implement a robocall solution. For instance, the Nomorobo service is not available for these customers. Despite these challenges, Frontier offers our customers other tools for filtering robocalls, including the following service features, all free of charge:

- Anonymous Call Rejection: Prevents callers who intentionally block their phone numbers, typical of robocalls, from getting through on the customer's phone line. All other calls will ring through as usual.
- Selective Call Rejection/Call Block: Allows customers to program their phone to block calls from any number they place on the rejection list. When this service is turned on, any callers on this list will hear an announcement that the customer is not accepting calls at this time. All other calls will ring through as usual.

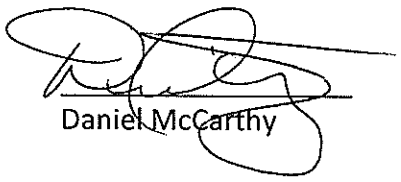
- Selective Call Acceptance: Allows customers to program phones to accept calls from a special list of callers. Customers also decide which calls ring through. Only callers on a selected list will ring through, while all other callers will hear an announcement saying calls are not currently being accepted.

In additions to these free tools, Frontier continuously reviews all possible industry solutions as they become available to evaluate their utility in fighting robocalls for both TDM and VoIP lines. If new solutions will benefit customers, Frontier has and will adopt them. For example, as stated in my November 19, 2018 letter to Chairman Pai, Frontier is committed to implementing SHAKEN/STIR for internet protocol calls by the end of this year – a solution that promises to greatly reduce robocall traffic.[1] And while the SHAKEN/STIR standard only directly applies to internet protocol calls, industry adoption will also help to significantly reduce illegitimate robocall traffic to TDM customers, particularly as more core infrastructure continues to migrate to VoIP.

Frontier also actively participates in the Industry Traceback Initiative, which is coordinated through USTelecom. Through this initiative, participating providers work together to identify sources of unlawfully spoofed calls and refer suspected fraud to the FCC and FTC for enforcement actions. These efforts have been lauded by the Commission as "invaluable" and "exactly the kind of industry/government cooperation necessary" to combat illegal robocalling and harmful spoofing.[2] Frontier also participates in the FCC's Do-Not-Originate initiative and blocks calls from numbers on the list.

We look forward to working with the Commission and the industry to continue the critical work of protecting consumers from unwanted robocalls. Please do not hesitate to contact me if you would like to discuss these important issues further.

Sincerely,



Daniel McCarthy

[1] *See Letter to Chairman Pai*, WC Docket No. 17-97 (Nov. 19, 2018).

[2] *See* Letter from Enforcement Bureau Chief Rosemary Harold and Chief Technology Officer Eric Burger to USTelecom (Nov. 6, 2018), *available at* https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf.

Google LLC
25 Massachusetts Avenue NW
Ninth Floor
Washington, DC 20001

202-346-1100 main
google.com

January 14, 2019

Via Email

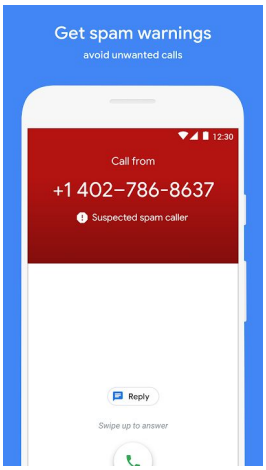
Jessica Rosenworcel
Commissioner
Federal Communications Commission
445 Twelfth Street SW
Washington, DC 20554

Dear Commissioner Rosenworcel:

We appreciate your December 12, 2018, letter acknowledging Google's efforts and coordination with the Commission on combating illegal robocalls. Google remains committed to implementing SHAKEN/STIR[1] once the standards are finalized and approved, and we have been deeply involved with the Secure Telephone Identity Governance Authority. Beyond supporting those industry-wide efforts, moreover, Google has led in providing consumers effective call authentication tools at no cost today.

For example, Google's Phone app (available at https://play.google.com/store/apps/details?id=com.google.android.dialer&hl=en_US) offers a robust solution for reducing the number of illegally spoofed calls to users on Android phones. The Phone app provides visual warnings about potential spam callers (see image below), enables users to block numbers on their own devices, and allows users to report suspicious calls to help protect the community from fraud and spam. Any mobile phone manufacturer and/or carrier can preload the Phone app on devices they sell, with no cost to them or to the users who benefit.

[1] SHAKEN/STIR is an acronym of two sets of technical specifications: the Secure Telephone Identity Revisited (STIR) protocols defined by the Internet Engineering Task Force (IETF), and the Signature-based Handling of Asserted information using toKENs (SHAKEN) specification defined by the ATIS/SIP Forum's IP-NNI Task Force.



In addition, users who have chosen Google's Android operating system can use Android to have their phone prevent suspected spam calls, including illegally spoofed calls, from ringing and instead send those calls immediately to voicemail. This feature, which is free, is optional to users and builds on the existing "suspected spam caller" warning feature in Android. For more information, please visit https://support.google.com/phoneapp/answer/3459196.

Most of Google's Pixel phones further offer a Call Screen feature, which gives users the option to have the Phone app ask who is calling and why, and to see a real-time transcript of the caller's response before deciding whether to answer a call. One tech publication has opined that "Call Screen is your best weapon against spam."[2] This tool is free to Pixel users. Google also offers it at no cost to manufacturers and carriers, who we welcome to adopt Call Screen on their phones. More details about Call Screen are available at https://support.google.com/phoneapp/answer/9118387.

Across our business, Google is doing what we can to help users avoid unwanted calls. We have developed the free solutions described above and reached out to carriers and manufacturers to encourage them to consider adopting our solutions for the benefit of their customers. We will continue to invest in our free solutions and to seek their wider distribution, while at the same time remaining committed to the deployment of STIR/SHAKEN.

Please contact me should you have any questions.

Respectfully submitted,

Darah Franklin
Counsel

[2] Patrick Holland, *Pixel 3's Call Screen and Now Playing Are the Best Reasons to Own This Phone: Besides the Camera, Of Course*, CNET, Dec. 12, 2018, https://www.cnet.com/news/pixel-3-call-screen-and-now-playing-are-the-best-reasons-to-own-this-phone/.

Charles W. McKee
Vice President, Government Affairs
Federal and State Regulatory

Sprint Corporation
900 7th Street NW, Suite 700
Washington, DC 20001
charles.w.mckee@sprint.com

Sprint

January 14, 2019

The Hon. Jessica Rosenworcel
Commissioner
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Commissioner Rosenworcel:

Thank you for your letter of December 12, 2018, regarding the Federal Communication Commission's ("FCC") efforts to combat the problem of illegal and unwanted robocalls. Sprint shares your goal of ending unlawful caller ID spoofing and empowering consumers with labeling and optional blocking services to combat illegal and unwanted robocalls.

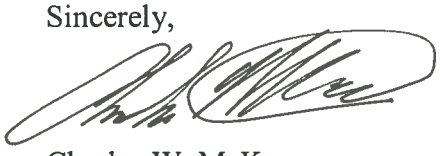
Sprint is proud to have been an industry leader in efforts to eradicate illegal and unwanted robocalls. Sprint participated in all four working groups of the FCC's 2016 Robocall Strike Force and co-chaired the "Empowering Consumer Choice" working group. Sprint was a part of the FCC's North American Numbering Council's Call Authentication Trust Anchor Working Group that led to the establishment of the SHAKEN/STIR Governance Authority.

Sprint has also worked with the industry and third parties to develop other strategies for addressing unwanted robocalls. Sprint has partnered with TNS and its Cequint mobile client subsidiary to develop an application for Sprint wireless customers that provides a robocall labeling and blocking service called Premium Caller ID. Premium Caller ID is available to almost all Sprint wireless customers for $2.99 per month. (Most devices sold in the last two years support Premium Caller ID, but certain customers with older mobile devices cannot use Premium Caller ID.) Premium Caller ID labels incoming robocalls and allows customers to selectively block calls based on risk level. TNS analyzes more than one billion call events per day across 400 carriers to identify nuisance and malicious calls. Premium Caller ID has processed hundreds of millions of calls for millions of Sprint customers and has categorized 64 million calls as being nuisance or malicious, thereby enabling Sprint's customers to block or decline to answer these calls.

While Premium Caller ID provides consumers a more flexible and advanced form of screening, Sprint customers have other options as well. Numerous third-party solutions, some free, are also available to Sprint customers through mobile application stores such as Google Play or Apple's App Store. Finally, all customers can configure their device to block specific individual numbers.

Thank you for your continued efforts and attention to this industry wide problem. Sprint remains committed to combating illegal and unwanted robocalls and will work with the FCC and the industry to develop and implement tools to resolve this problem.

Sincerely,



Charles W. McKee
Vice President Government Affairs
Federal and State Regulatory

T-Mobile USA, Inc.
601 Pennsylvania Avenue, Washington, DC 20004

January 14, 2019

Hon. Jessica Rosenworcel
Commissioner
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Commissioner Rosenworcel:

Thank you for your December 12, 2018 letter to our CEO, John Legere, calling on carriers across the country to offer free tools to help combat unwanted robocalls. T-Mobile USA, Inc. ("T-Mobile")[1] agrees with you that robocalls represent a growing problem. That is why, as the Un-carrier, T-Mobile is leading the industry in fighting fraud by providing our customers tools they love to stop the robocalls they hate.

We have been, and will continue to be, a leader in finding innovative solutions to help our customers avoid illegal and unwanted robocalls. For instance, we have been an active participant in key industry groups aimed at combatting unwanted robocalls—the FCC Robocalling Strike Force,[2] the ATIS STI-GA Board,[3] and the USTelecom Industry Traceback Group.[4] And as we recently stated in a letter responding to Chairman Pai, we were the first carrier to announce readiness to launch industry call-authentication protocols known as Secure Telephone Identity Revisited ("STIR") and Signature-based Handling of Asserted Information Using toKENS ("SHAKEN").[5] We are also happy to share with you today that we have just rolled out to

---

[1] T-Mobile USA, Inc. is a wholly-owned subsidiary of T-Mobile US, Inc., a publicly traded company.
[2] *Statement of Chairman Wheeler on Progress Toward Offering Consumer Robocall Blocking Choices*, FCC (July 25, 2016), https://docs.fcc.gov/public/attachments/DOC-340458A1.pdf. In addition to T-Mobile, the other 15 Members of the Robocall Strike Force were AT&T, Apple, Bandwidth.com, Birch, Blackberry, British Telecom, CenturyLink, Charter, Cincinnati Bell, Comcast, Cox, Ericsson, FairPoint, Frontier, GENBAND, Google, Inteliquent, Level 3, LG, Microsoft, Nokia, Qualcomm, Rogers, Samsung, SilverStar, Sirius/XM, Sprint, Syniverse, US Cellular, Verizon, West, and Windstream.
[3] Marcella Wolfe, *Secure Telephone Identity Governance Authority Launched in Major Industry Effort to Combat Unwanted Robocalling*, ATIS (Sept. 18, 2018), https://sites.atis.org/insights/secure-telephone-identity-governance-authority-launched-in-major-industry-effort-to-combat-unwanted-robocalling/. The Secure Telephone Identity Governance Authority Board is managed by the industry under the auspices of ATIS and held its first Board meeting in August 2018.
[4] *See* Chloe Sanchez, *Taking Charge Against Robocalls*, USTELECOM (Sept. 26, 2018), https://www.ustelecom.org/blog/taking-charge-against-robocalls. USTelecom has led the 24-member Industry Traceback Group since 2016 to identifying the source of illegal robocalls and working with law enforcement to bring them to justice.
[5] Letter from Kathleen O'Brien Ham, Senior Vice President, Government Affairs, T-Mobile USA, Inc., to Hon. Ajit V. Pai, Chairman, FCC, WC Docket No. 17-97 (filed Nov. 19, 2018).

customers our "Caller Verified" technology, which, for now, implements STIR/SHAKEN standards for calls made to Samsung Note9 smartphones on the T-Mobile network. These standards combat illegal caller ID spoofing, such as the current scam referred to as "neighbor spoofing," in which scammers temporarily hijack a phone number to match the area code and three-digit prefix of the person they are targeting, making the incoming call look familiar. This means that for customers with these devices "Caller Verified" will appear when an incoming call is authentic and that the phone number has not been hijacked by scammers and spammers. This technology is free for all Un-carrier customers and will be made available on more smartphones later this year. Once the other wireless carriers implement STIR/SHAKEN, Caller Verified will work on calls made across networks.

We agree with you that consumers should have tools to combat robocalls, so we have led the way by providing those tools to our customers for free, and our customers love these services. T-Mobile offers two free services—Scam ID and Scam Block—to all postpaid T-Mobile customers and Metro customers. These network-based services are automatically activated on all phones with caller ID; because they are automatically activated at the network level, customers need not install software or apps, or perform any handset configuration to use the services. Scam ID identifies calls that are likely to be malicious or spoofed by displaying "Scam Likely" on the handset. Scam Block goes beyond Scam ID by providing T-Mobile customers the option to block calls that are identified as fraudulent at the network level so that they never reach their handset. T-Mobile is still the only major wireless provider to deliver free scam protection on any device without requiring an app or registration. Since launching Scam ID and Scam Block in April 2017, we have identified over 7.2 billion calls as "Scam Likely" and blocked over 1.7 billion scam calls.

Customers can turn Scam ID off online at mytmobile.com, via the T-Mobile app on their devices, or by calling Customer Care. Most customers do not turn off the feature, however, because they quickly realize it is a valuable service that allows them to make an informed choice about whether to answer a call that has been identified as "Scam Likely." Customers can switch Scam Block on and off through the Name ID application, or by dialing a three-digit short code on their handsets or calling Customer Care.

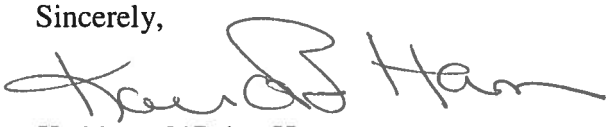
In addition to Scam ID and Scam Block, all customers on T-Mobile One Plus plans receive Name ID, which is our caller ID service, for free. Customers on other monthly service plans may pay $3.99 per month for the service. Name ID is pre-loaded on every new Android device so that customers can try it out for 30 days for free and then decide whether to sign-up.

In addition to leading the way on implementation of STIR/SHAKEN standards, T-Mobile has enhanced Scam ID and Scam Block with a "call printing" feature that helps to detect spoofed robocalls. Third-party call blocking apps are largely ineffective when it comes to detecting scam robocalls because they can only black-list against known scam numbers, not legitimate numbers that are momentarily hijacked by scammers. In contrast, call printing provides real-time

decisions on incoming calls, intelligent analysis of phone call and network-wide data, and an adaptable machine-learning based framework to stop the next scammer tactic.[6]

We are proud of being the industry leader on scam identification and blocking and look forward to continuing to work with you and the Commission in the fight to protect American consumers against robocalls.

Sincerely,



Kathleen O'Brien Ham,
Senior Vice President, Government Affairs

[6] Comments of First Orion Corp., CG Docket No. 17-59, at 2-3 (filed Sept. 24, 2018).

January 14, 2019

Via Electronic Mail

The Honorable Jessica Rosenworcel
Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Dear Commissioner Rosenworcel:

On behalf of TDS Telecommunications LLC ("TDS Telecom"), thank you for your letter of December 12, 2018. We share your view that "[e]very American should have access to a phone system they can trust," and to that end, together with you and other leaders in the public and private sectors, we seek to eliminate unlawful and unwanted robocalls.

TDS Telecom, which is headquartered in Madison, Wisconsin, is committed to the highest standards of service for our customers. We provide connectivity to customers in nearly 900 rural, suburban and metropolitan regions throughout the United States, and we take seriously our commitment to serve these customers reliably, safely and lawfully. Taking action to protect our customers from unlawful robocalls—without undermining legitimate call completion—is a core part of that commitment.

At one time, customers relied heavily on caller ID tools as a means of screening out—and in some cases, electing not to receive—unwanted robocalls. Unfortunately, the rise in caller ID spoofing has rendered these tools less effective. TDS Telecom has and continues to explore call identification and blocking technologies currently available in the marketplace. For example, TDS Telecom has worked with multiple vendors that market call authentication solutions to explore alternatives that would enable it to reliably detect spoofing. Unfortunately, the Caller ID-based solutions reviewed to date appear easily defeated by techniques such as neighbor spoofing. Because of these drawbacks, TDS Telecom has not deployed these solutions.

TDS Telecom remains committed to finding and employing solutions to improve our customers' experience. As discussed in our response to FCC Chairman Ajit Pai's letter in November, TDS Telecom has committed to testing a SHAKEN/STIR solution in our IP networks this year. As part of that project, TDS Telecom also will test currently available call identification and blocking technologies in both our TDM and IP networks.

This commitment to testing a range of solutions reflects our view that solving the problem of unlawful robocalls likely will require a combination of technologies and timetables. This is particularly the case for those carriers, like TDS Telecom, that serve less densely-populated (and thus more costly) areas and have a network consisting a hybrid of IP- and TDM-

based technologies to deliver critical communications services to rural consumers, businesses, and other institutions.

Thank you again for your letter. If I can provide additional information about TDS Telecom's efforts to eliminate the problem of unlawful robocalls, please do not hesitate to let me know.

Respectfully submitted,

Andrew Petersen
Sr. Vice President – Corporate Affairs

U.S. Cellular

January 14, 2019

Ms. Jessica Rosenworcel
Federal Communications Commission
Washington, D.C. 20554

Dear Commissioner Rosenworcel,

Your letter of December 12, 2018 to Kenneth Meyers, the Chief Executive Office of U.S Cellular Corporation ("U.S. Cellular"), has been forwarded to me for a response. U.S Cellular shares your concern about the proliferation of illegal robocalls and that is why we are so excited about the promise of the SHAKEN/STIR protocol to substantially reduce the number of illegal robocalls. We are aggressively moving to deploy SHAKEN/STIR in our network during the second half of 2019. While everyone would, understandably, like to see this capability deployed sooner the fact is that this is a complicated undertaking that requires promulgation of industry standards, negotiation of vendor contracts and the implementation across the industry for maximum effectiveness. I am attaching our recent response to Chairman Pai concerning the status of our SHAKEN/STIR efforts.

In the meantime, U.S. Cellular provides other tools and capabilities at no charge that consumers may find helpful in combating the problem of illegal robocalls. These include access to Call Guardian, a robocall and call identification application that is pre-loaded on many of our devices. Call Guardian is a free application, provided by a company called Cequint, that provides an on-device warning to consumers when an incoming call is likely a scam or spam call. If the call is presenting a phone number that is one of the 5,000 numbers Cequint has determined to be very likely a scam or spam call, the consumer is alerted and can decide if they would like to receive the call, or ignore it. Cequint utilizes a proprietary algorithm to identify these phone numbers, and the list is actively updated. Additional features and capabilities are available with Call Guardian as part of a subscription offering for $3.99 per month.

U.S. Cellular also provides consumers with helpful suggestions about how to deal with illegal robocalls on our website, including a link to the national Do Not Call Registry. You can review this information at the following link; www.uscellular.com/robocall. Our website also includes links for consumers to access operating tutorials for each of the devices we sell, including procedures for blocking inbound calls from specific telephone numbers. Our customer support specialists are also happy to answer questions our customers may have about how to reduce the number of robocalls they receive.

Between educating consumers about the tools that are available today, implementation of the call authentication network protocol known as SHAKEN/STIR, and increased enforcement by the FCC and FTC of existing laws against robocall violators, we believe progress is being made to address the plague of unwanted and illegal robocalls. We look forward to continued cooperation with the FCC and the industry on this matter of great importance to customers.

Sincerely,

John Gockley
Vice President
Legal & Regulatory Affairs

Kathleen M. Grillo
Senior Vice President
Public Policy & Government Affairs
1300 I Street, NW, Suite 500E
Washington, DC 20005
Phone: 202-515-2533
Kathleen.m.grillo@verizon.com

January 14, 2019

The Honorable Jessica Rosenworcel
Commissioner
Federal Communications Commission
Washington, D.C. 20554

Dear Commissioner Rosenworcel:

Thank you for your recent letter to Verizon CEO Hans Vestberg about the importance of free tools consumers can use to insulate themselves from the incessant flow of unwanted and illegal robocalls. We know our customers hate these calls and we are taking aggressive steps on multiple fronts, summarized below, to address this growing problem.

While ultimately the robocall problem needs to be addressed by stopping illegal robocalls at the source and by implementing technology to prevent bad actors from disguising their identities, Verizon agrees that customers also deserve ways to protect themselves from robocalls. To that end, we provide tools that wireless and wireline customers can use to help insulate themselves from unwanted and illegal robocalls, and we empower our customers to use options available from third parties.

Verizon's Robocall Detection and Blocking Toolsets

More than a year ago, Verizon added robocall protection features for no additional charge to wireless customers subscribing to our Call Filter service ($2.99/month).[1] For all incoming calls, the service provides caller ID information and an innovative risk meter that explains the level of risk associated with the call. If a call meets Verizon's spam criteria, the incoming call screen will display a spam label. Customers also have the option to send directly to voicemail any spam calls falling into the risk category they choose to block and can look up identified spam numbers in our database. As we enhance our robocall protection features, we are also evolving our pricing for the features that are most important to our customers – spam detection and blocking. We currently offer free alerts about potential spam calls to customers with certain Android phones, and we will begin rolling out free spam alerting and blocking to all of our customers whose smartphones support those features starting in March.

[1] *See* https://www.verizonwireless.com/support/call-filter-faqs/. The service was previously called Caller Name ID.

On the wireline side, all Verizon customers with Caller ID service, whether they are served over fiber or copper facilities, receive Verizon's Spam Alerts service for free.[2] The caller ID displays show "SPAM?" before a caller's name if the calling number matches Verizon's spam criteria. Since its launch last year, this feature has alerted Verizon customers about nearly a billion malicious robocalls. Verizon also makes sure its Fios Digital Voice customers are aware of the free blocking service offered by Nomorobo, which relies on the simultaneous ring feature that we provide for free to those customers. We have worked with Nomorobo to implement a "one click" feature to enable our customers to efficiently sign up with its service if they choose to do so.

Stopping Robocalls at the Source and Restoring Trust in Caller ID

Verizon is an industry leader on multiple initiatives to address the spoofing problem and to root out illegal robocallers at the source. Blocking solutions cannot fully resolve the robocall problem because it is easy for spammers to use computers to call large numbers of consumers while disguising their identities by changing the "calling party number" of their calls to make it seem like they are coming from a different number. That practice is called "spoofing." In most cases, Verizon cannot identify the illegal robocaller because the spoofed robocalls typically start with Internet-based providers (often internationally), and then pass through several other companies' networks before reaching Verizon. So Verizon usually has no way to tell who made the calls unless each of those "upstream" carriers agrees to provide information about where the calls are coming from – and unfortunately our attempts to trace back suspicious traffic often dead-end when one of those upstream companies in the call path refuses to cooperate. Verizon's work addressing these challenges includes:

- Verizon has implemented programs to prevent our services from being used by illegal robocallers. We are encouraging other voice service providers to implement similar "know your customer" programs and have encouraged the Commission to take action against providers that do not implement appropriate practices both to trace back illegal traffic and to avoid originating it in the first place.
- Verizon is committed to deploying the new "STIR/SHAKEN" call authentication technology to protect consumers from spoofed calls. This technology will help service providers evaluate whether a call is spoofed. We have invested substantial amounts of time and resources upgrading our networks with the STIR/SHAKEN technology.
- Verizon is a founding member of the USTelecom Industry Traceback Group, an industry-led organization that traces back suspicious robocall traffic and stops many illegal robocalls. Since we and two other service providers founded the group two years ago, over twenty more have joined us. While these activities obviously have not solved the problem, the flood of illegal robocalls would be even greater without them.[3]

---

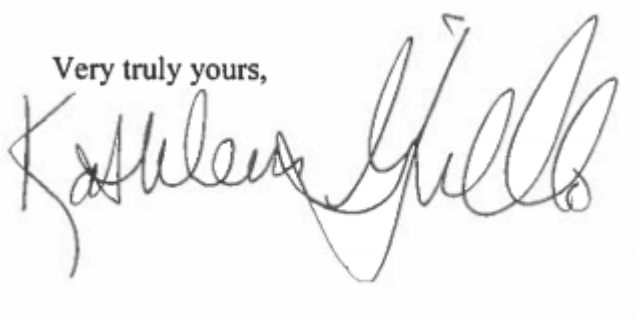
[2] *See* http://www.verizon.com/about/news/block-spam-robocalls-with-verizon-new-tool.

[3] *See* Letter from Rosemary C. Harold, FCC, to Jonathan Spalter, USTelecom (Nov. 6, 2018), (*available at* https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf).

- We support stronger federal laws to outlaw improper spoofing. Few robocallers get charged with illegal spoofing because under the Truth in Caller ID Act, the government currently must prove that the caller intended to defraud, cause harm, or illegally obtain something of value. Verizon supports a simple rule that would make it illegal for any caller to use any phone number that it is not authorized to use. Verizon also supports legislation requiring service providers to deploy the STIR/SHAKEN call authentication technology.

Thank you again for your strong commitment to addressing this important issue. Please know that Verizon fully appreciates the harm caused by robocalls and we are committed to working on multiple fronts to better protect our customers.

Very truly yours,



January 14, 2019

Commissioner Jessica Rosenworcel
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Tools to Combat Robocalls

Dear Commissioner Rosenworcel:

I appreciate the opportunity to respond on behalf of Vonage Holdings Corp. to your questions directed to our CEO, Alan Masarek, regarding the solutions we offer to consumers to combat unwanted robocalls. We share your concern about the impact that a rising tide of scam calls is having on consumers, and we are committed to giving our customers cutting-edge tools to control the kinds of calls they receive.

As I explained in my November 19, 2018 letter to Chairman Pai, Vonage has developed plans to implement the SHAKEN/STIR framework in 2019 and is collaborating with industry partners to develop the policies and systems needed to authenticate calls. We are making significant investments throughout our network today to ensure that our customers get the benefits of authenticated caller ID as soon as possible. We recognize, however, that even these expedited efforts cannot address the problems consumers experience today. That is why we have taken a multifaceted approach, working with industry-leading vendors, to combat unwanted calls.

For business customers, we offer Spam Shield, a Vonage offering that checks incoming calls against a dynamic database of numbers associated with telemarketing, robocalls, and scams. If Spam Shield finds a match, it displays "suspected spam" on the customer's caller ID and allows them to decline the call and block future calls from that number. Spam Shield leverages technology developed by Nomorobo, which won the Federal Trade Commission's Robocall Challenge in 2013 for Best Overall Solution for blocking illegal robocalls. While "blacklist" solutions like Spam Shield cannot prevent all unwanted calls, they are helping to combat the problem today and will complement verified caller ID solutions in the future. We make this service available to Vonage Business customers at a cost of $2.99 per month per extension (plus taxes and fees). That fee covers the per-call fee that Vonage pays to Nomorobo.

Vonage also offers services that allow business and residential customers to identify names and phone numbers of calls they receive. To provide consumers with the most accurate caller ID information available today, Vonage contracts with Neustar, which queries its internal database and external sources of caller information. Vonage pays Neustar each year for this caller ID

service, which is included in the price of our business and residential plans. Using this information, customers can use our blocking options to block future calls. We offer:

- **Anonymous Call Block** – Blocks calls from callers that block recipients from receiving caller ID information and plays a message indicating that the called party does not answer calls from unknown numbers. For business customers, this feature can be enabled by administrators across an organization.

- **Selective Call Block** – Allows end users or administrators to select individual phone numbers or number patterns (for example, numbers from a particular area code) to block using the Vonage Extensions app or online account. Numbers can be blocked and unblocked at any time.

- **Do Not Disturb** – Temporarily stops all incoming calls from ringing and directs callers to voicemail or a message that the called party is not accepting calls.

We share your concern, and we appreciate the Commission's work to promote tools that combat scam calls, caller ID spoofing, and unwanted robocalls. I would be pleased to answer any additional questions you may have. Please do not hesitate to contact me at 732-444-4613.

Respectfully,

Randy K. Rutherford
Chief Legal Officer
Vonage Holdings Corp.
23 Main Street
Holmdel, NJ 07733

CC: Alan Masarek, CEO of Vonage Holdings Corp.