Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and	)	CG Docket No. 17-59
Eliminate Unlawful Robocalls	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

Comments
of

Consumer Reports
National Consumer Law Center, on behalf of its low-income clients
Consumer Action
Consumer Federation of America
National Association of Consumer Advocates
Public Knowledge

July 24, 2019

It's time for swift action on robocalls—the unwanted, autodialed calls that not only annoy and harass us and interfere with our peace of mind, but wake up night shift workers during the day, and interrupt caregivers and sick patients when they are trying to recover. Seniors tell us that they have fallen when rushing to catch the phone. Robocalls to cell phones pose additional safety risks when they interrupt consumers when they are driving. Consumers need better options than to be told to just "hang up." The above-listed groups appreciate the recent steps that the Federal Communications Commission (FCC) has taken in order to address harmful calls, including the recent order clarifying that phone companies can block suspicious calls on an opt-out basis,[1] and efforts to prompt the major voice service providers to implement SHAKEN/STIR protocols by the end of 2019.[2] Yet as of mid-2019, most of these companies have not fully adopted SHAKEN/STIR, and robocalls are still at record levels.[3] Consumers should have effective protections from robocalls by default. To secure this, the FCC should:

- Require phone companies to adopt effective call-authentication policies and technologies, at no additional line item charge to subscribers, by June 1, 2020;
    - Originating providers should be required to know who is placing the traffic and should decline traffic from bad actors;
    - For the majority of phone service providers who have the capability to implement SHAKEN/STIR, that technology should be implemented immediately;
    - For those providers who do not have that capacity, alternative techniques should be identified and applied on an expedited basis.
- Require phone companies to provide three levels of call blocking options: opt-out screening of scam calls, opt-in to more comprehensive technologies to block spam calls, and personal blacklists, all at no additional line item charge to subscribers;
- Develop policies for improperly blocked calls that leave call recipients in control, including limiting a "critical calls" whitelist to authenticated, genuine emergency calls only, and a separate unblocking system, created by the FCC, guided by a specific set of criteria, and paid for by the members of the calling industry who seek to benefit from using it.

This comment is focused on technological approaches to help address the unwanted call problem. These techniques will be particularly useful in combating fraudulent calls, for which

[1] Fed. Commc'ns Comm'n, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, CG Docket No. 17-59, WC Docket No. 17-19 (June 7, 2019), https://ecfsapi.fcc.gov/file/0607046191409/FCC-19-51A1.pdf.
[2] *Chairman Pai Calls on Industry to Adopt Anti-Spoofing Protocols to Help Consumers Combat Scam Robocalls*, Fed. Commc'ns Comm'n, Nov. 5, 2018, https://docs.fcc.gov/public/attachments/DOC-354933A1.pdf.
[3] Youmail Robocall Index, Historical Robocalls by Time, (last visited July 21, 2019), https://robocallindex.com/history/time. Youmail shows that as of June 2019, U.S. consumers had received 29 billion robocalls this year to date. In 2018, U.S. consumers received nearly 48 billion robocalls in the entire year.

enforcement efforts have so far been wholly inadequate. But in no way will these techniques serve as a substitute for strong rules that protect consumers from all unwanted calls. Though some in the calling industry have incorrectly argued otherwise,[4] scam robocalls are far from the only kind of unwanted robocalls. If the FCC weakens the robocalls rules, as the U.S. Chamber of Commerce and the calling industry have urged them to do,[5] then consumers will receive an even higher percentage of unwanted robocalls from debt collectors and telemarketers.

According to the most recent YouMail data, telemarketing and debt collection calls make up about half of the robocalls that consumers receive.[6] Consumers are fed up with these calls as well. TNS, the call-analytics company, reports that debt collection calls are rated extremely negatively.[7] The CFPB reported that one in four consumers feels threatened by debt collectors, and that most debt collectors do not stop calling, even if the consumer has asked them to stop.[8]

While scam calls are far from the only type of unwanted robocalls received by consumers, they pose unique challenges to enforcement efforts. Many of these callers hide their identities using caller ID spoofing. Some quickly change the number displayed on the caller ID, or mimic a local number currently in use, so it is nearly impossible for consumers to block them one-by-one.[9]

Because it is difficult for phone companies to determine and verify the identity of a spoofed call in real-time as it is coming through the network,[10] spoofed calls are too often able to evade blocking mechanisms. Spoofed calls also victimize the consumer whose number is spoofed. We

[4] *See*, e.g., Comments of the American Association of HealthCare Administrative Management, CG Docket No. 17-59 at 1-2 (Jul. 20, 2018), https://ecfsapi.fcc.gov/file/10720929113148/AAHAM%20Robocalling%20PN%20Comments%20(07-20-2018).pdf; Comments of Professional Association for Customer Engagement (PACE) at 2 (Jul. 20, 2018), https://ecfsapi.fcc.gov/file/10720128858463/PACE%20TCPA%20Comment%20to%20FCC%20(7-20-18).pdf.
[5] U.S. Chamber Institute for Legal Reform et al., Petition for Declaratory Ruling, CG Docket No. 02-278 (filed May 3, 2018), https://ecfsapi.fcc.gov/file/1051094891940/Petition%20for%20Declaratory%20Ruling.pdf; Comments of Professional Council for Consumer Engagement, CG Docket No. 02-278 and 18-152 (Jun. 13, 2018), https://ecfsapi.fcc.gov/file/106130429322839/PACE%20TCPA%20Comment%20to%20FCC%20(6-13-18).pdf.
[6] YouMail, YouMail Robocall Index, June 2019, https://robocallindex.com/.
[7] Comments of TNS, CG Docket No. 17-59 at 6-7 (Jul. 20, 2018), https://ecfsapi.fcc.gov/file/10720017728535/TNS%20COMMENTS%20ON%20FCC%20PUBLIC%20NOTICE%20CG%20Docket%20No.%2017-59.pdf.
[8] Consumer Fin. Protection Bureau, *CFPB Survey Finds Over One-In-Four Consumers Contacted By Debt Collectors Feel Threatened* (Jan. 12, 2017), https://www.consumerfinance.gov/about-us/newsroom/cfpb-survey-finds-over-one-four-consumers-contacted-debt-collectors-feel-threatened/.
[9] Fed. Commc'ns Comm'n, *Caller ID Spoofing* (July 15, 2019), https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.
[10] Fed. Trade Comm'n, *Robocalls: All the Rage, An FTC Summit* at 127-128 (Oct. 18, 2012), https://www.ftc.gov/sites/default/files/documents/public_events/robocalls-all-rage-ftcsummit/robocallsummittranscript.pdf.

have heard from consumers who receive dozens of calls from angry neighbors because they have received calls spoofed with the consumer's number.[11]

Caller ID verification procedures, such as SHAKEN/STIR, have a great deal of promise for addressing the scam robocall problem, but only if the FCC takes the lead to guide compliance, and establishes appropriate policies that address the root of the problem: that phone companies aren't currently responsible for knowing who their customers are, and some originating phone companies are placing harmful traffic into the network. Below, we develop on these points in more detail.

The FCC should require phone companies to adopt effective call-authentication policies and technologies, at no additional line item charge to subscribers, by June 1, 2020.

It is time to set real deadlines for call authentication. While the FCC has pressed the major voice service providers to implement call authentication technology SHAKEN/STIR by the end of this year, cross-carrier implementation has been relatively limited by mid-2019.[12] And some major landline carriers have declined to provide specific estimates for when they plan to begin authenticating calls.[13] Consumers are demanding action, now: nearly 230,000 consumers signed a Consumer Reports petition to the FCC demanding free, effective caller ID authentication technology. This idea is gaining acceptance among policymakers, as evidenced by legislation progressing rapidly through Congress that would require effective caller ID authentication.[14] The deadline for major voice service providers to comply should be June 1, 2020.

<u>Originating providers should be required to know who is placing the traffic and should decline traffic from bad actors.</u>

The FCC should also guide compliance and establish appropriate policies with respect to call authentication. For example, the FCC should require originating providers know who is originating the call and to hold them accountable to decline fraudulent traffic. As AT&T noted in the recent SHAKEN/STIR summit, "focusing in on those service providers who are originating those calls, and finding a way to require them to implement SHAKEN/STIR or stop carrying the traffic or whatever it is, that's going to have the biggest, quickest impact."[15] The specific

[11] This has been documented online as well, through online phone company forums. See AT&T Community Forum, "My phone number has been spoofed - what can I do to fix this?" https://forums.att.com/t5/Wireless-Account/My-phone-number-has-been-spoofed-what-can-I-do-to-fix-this/td-p/5237736.
[12] *T-Mobile and Comcast First to Give Customers New Anti-Robocalling Feature*, T-Mobile (April 17, 2019), https://www.t-mobile.com/news/inter-carrier-stir-shaken-launch.
[13] See, Letter from TDS Telecom to the Honorable Ajit V. Pai, Nov. 18, 2018, https://ecfsapi.fcc.gov/file/11190057404723/TDS%20Nov.%2019%202018%20letter.pdf.
[14] S. 151 (2019); H.R. 3375 (2019).
[15] Linda Vandeloop, AT&T, SHAKEN/STIR Robocall Summit, Jul. 11, 2019, https://www.fcc.gov/SHAKENSTIRSummit (at approximately 50.10).

technologies that are used to actually authenticate identities and share that information with other carriers are less important, especially as no single current technology will be entirely effective in addressing unwanted robocalls, and will likely have to be supplemented by alternative techniques. For example, SHAKEN/STIR does not allow traditional landline providers to sign calls, and its efficacy is limited with respect to calls originating overseas. Whatever specific technologies are used, they should be effective in eliminating deceptively spoofed calls in the network.

For those providers who do not have the capacity to implement SHAKEN/STIR, alternative techniques should be identified and applied on an expedited basis.

All phone companies must be required to comply with call authentication techniques, not just the major carriers. As a representative of robocall-mitigation service TNS noted at the SHAKEN/STIR summit, "A lot of the tier ones do not generate the bad traffic. About 87% of the bad traffic comes from carriers outside of the tier one."[16] Small and rural carriers should be allowed flexibility with respect to deadlines; but the FCC should identify and take the steps necessary to enable full participation, and reassess the impact of these allowances each year.

In the meantime, effective alternative techniques should be identified, and their use should be encouraged or required by the FCC as appropriate. The FCC and phone companies should think creatively about techniques to verify the source of calls and eliminate traffic tied to bad actors, rather than being tied to a specific technology or methodology.

The multiple number problem: require full attestation.

The FCC should require phone companies employing SHAKEN/STIR to sign calls with full attestation—the highest level of attestation—by the June 1, 2020 deadline. Full attestation applies to calls in which the phone company knows who initiated the call and who owns the number.[17] This is especially important to solve the related problem caused by the fact that scammers and others can simply buy many different numbers, and then authenticate those numbers. The call would appear to be legitimate, even if it is fraudulent. This could be even more damaging than if SHAKEN/STIR were not used at all, as consumers would be more likely to trust a call that appears verified, even if its content is fraudulent.

[16] Lavinia Kennedy, TNS, SHAKEN/STIR Robocall Summit, Jul. 11, 2019, https://www.fcc.gov/SHAKENSTIRSummit. Tier One includes AT&T, Verizon, CenturyLink, and Sprint. Tier Two carriers must purchase access to Tier One networks, and includes Comcast and Cox. CTS Telecom, Inc., *The Three Tiers of ISPS: What they Mean and Why They're Important* (last visited July 21, 2019), https://www.ctstelecom.com/the-three-tiers-of-isps-what-they-mean-why-theyre-important/.

[17] TransNexus, *Understanding SHAKEN/STIR*, (last visited July 21, 2019), https://transnexus.com/whitepapers/understanding-stir-shaken/.

The FCC should require participation in the traceback program.

To supplement call authentication strategies, the FCC should require participation in a government-supervised traceback program, and phone companies should be required to decline traffic from providers that do not participate. Since calls are typically routed through multiple phone companies before they reach the recipient, it has often taken months in order to trace a complaint about a call back to the originating carrier, as the enforcement agency has had to seek multiple subpoenas to obtain the necessary information.[18] The traceback program has routinized this process and has sped it up, in many cases, to a matter of days.[19] If all providers were participating in the program, the process would be even more successful. Enforcement authorities could more quickly identity perpetrators and shut down the traffic. Having the phone companies decline traffic from bad actors would also reduce the amount of fraudulent traffic in the system.

Full participation in the traceback program will also help address fraudulent international calls. As Verizon noted at the SHAKEN/STIR summit, "Our encouragement would be to use traceback robustly particularly on the international side."[20] SHAKEN/STIR currently does not protect effectively against calls originating internationally, since it depends on the participation of originating carriers. Even if the FCC mandates SHAKEN/STIR implementation, its authority does not extend to carriers outside of the United States. This is a problem because according to the FTC, many illegal robocalls originate overseas.[21] Thus, traceback is likely to be a key component in effectively addressing fraudulent traffic originating internationally.

The FCC should ensure that call authentication techniques maintain consumer privacy.

In addition, anti-robocall efforts are fundamentally privacy initiatives, and call authentication techniques should not be used to undermine the legitimate privacy interests of consumers as they make calls. There are legitimate reasons to obscure the caller ID information for certain kinds of calls, and consumers should always have the option to decline to transmit it to the call recipient. The TCPA and FCC rules protect the ability of callers to suppress their caller ID information.[22] The FCC has indicated that SHAKEN/STIR has the ability to indicate that the caller ID information has been verified by the provider without sending the full caller ID information to

[18] Report on Robocalls, CG Docket No. 17-59 at ¶ 29-31 (Feb. 2019), https://docs.fcc.gov/public/attachments/DOC-356196A1.pdf.
[19] Linda Vandeloop, AT&T, SHAKEN/STIR Robocall Summit, Jul. 11, 2019, https://www.fcc.gov/SHAKENSTIRSummit.
[20] Jeff Haltom, Verizon, SHAKEN/STIR Robocall Summit, Jul. 11, 2019, https://www.fcc.gov/SHAKENSTIRSummit (at approximately 1:07).
[21] *Abusive Robocalls and How We Can Stop Them, Before the U.S. Senate Comm. on Commerce, Science, and Transportation, 115th Cong*. at 1 (2018) (testimony of the Fed. Trade Comm'n), https://www.ftc.gov/system/files/documents/public_statements/1366628/p034412_commission_testimony_re_abusive_roboc alls_senate_04182018.pdf.
[22] 47 U.S.C. § 227(e)(2); 47 C.F.R. §64.1604(b).

the call recipient.[23] The FCC should require SHAKEN/STIR, as well as other authentication technologies, to have that functionality.

The FCC should ensure that consumer voices are represented in SHAKEN/STIR governance.

As noted above, specifying the technologies used to address scam calls, including those that have been deceptively spoofed, is less important than ensuring the effectiveness of the policies that guide the system—for example, requiring that the originating provider should know the identity of the call originator. Thus, it is essential that those most affected by robocalls—consumers—are represented in the governance of SHAKEN/STIR. The FCC should set guidelines for the implementation of caller ID authentication and, at the very least, ensure that a consumer representative is on the governance board that manages SHAKEN/STIR.

Currently, the industry is taking the lead in managing SHAKEN/STIR.[24] As Henning Schulzrinne, former Chief Technology Officer of the FCC, noted in his Minority Report to the North American Numbering Council's Report on Caller ID authentication, as this effort to address robocalls has been largely spurred by consumer outcry, their interests should be represented as well.[25] He further noted that specialized technical expertise is not required in order to participate meaningfully on the governance board.[26] The FCC should ensure that consumer voices are represented on the board.

The FCC must closely oversee compliance with call authentication requirements and regularly assess their efficacy.

The FCC also has an important role to play in ensuring that companies are complying with call authentication requirements and that they are effective. The FCC should make public who has been granted an extension on implementing caller ID authentication, why they were granted an extension, the extent to which these carriers are originating bad traffic, and whether calls originating from carriers with those exemptions are regularly being blocked. This should be one component of a much broader analysis of the efficacy of the anti-robocall effort. The FCC should regularly collect and publish information about compliance with authentication, the origins of bad traffic, the volume of robocalls, type of call, percentage blocked, number of calls improperly blocked, and complaints.

---

[23] Fed. Commc'ns Comm'n, Call Authentication Trust Anchor, Notice of Inquiry (July 14, 2017) at ¶ 43, available at https://ecfsapi.fcc.gov/file/07141096201120/FCC-17-89A1.pdf.
[24] Letter from ATIS to FCC Commissioners (Sept. 13, 2018), https://ecfsapi.fcc.gov/file/10913940405809/STIGA%20Letter%20to%20the%20FCC%209.13.18.pdf.
[25] NANC Call Authentication Trust Anchor Working Group, *Report on Selection of Governance Authority and Timely Deployment of SHAKEN/STIR* at 24-25 (May 18, 2018), http://www.nancchair.org/docs/mtg_docs/May_18_Call_Authentication_Trust_Anchor_NANC_Final_Report.pdf.
[26] *Id.*

The FCC should require phone companies to provide three levels of call blocking options: opt-out screening of scam calls, opt-in to more aggressive, advanced technologies to block spam calls, and personal blacklists, all at no additional line item charge to subscribers.

It is not sufficient for caller ID authentication and associated services to simply indicate the accuracy of the caller ID information. Just as Caller ID has not stopped the scourge of robocalls, simply providing more information to consumers will fail to address much of the harm associated with robocalls, which is the unwanted interruption coming from the ringing telephone. Caller ID authentication will give phone companies more confidence in intercepting scam calls, but it must be paired with effective mechanisms to allow the phone companies screen out these calls and at no additional charge—for example, redirecting the calls to voicemail or to a separate "spam" folder that consumers can review later at their convenience.

Opt-out screening for scam calls

Phone companies should be required to screen out suspected scam robocalls on an opt-out basis. While the FCC appropriately reaffirmed last month that phone companies *may* offer advanced call-blocking tools on an opt-out basis, phone companies are not required to do so.[27] And carriers' responses to Commissioner Starks's request for information about the availability of call-blocking tools suggest that of the major carriers, only AT&T is currently offering this service.[28] As Commissioner Starks notes, it is also important that these tools are offered at no additional line item charge for consumers.[29]

Opt-in screening for spam calls

Phone companies should also be required to offer advanced technologies with more comprehensive blocking capabilities to screen out spam calls on an opt-in basis, at no additional line item charge. The FCC has made clear that phone companies have the full authority to offer these services, that will block entire categories of robocalls, regardless of whether they are legal or not.[30] Those tools should give consumers flexibility in terms of the categories of calls they would like to block, such as debt collection or telemarketing calls. Currently, AT&T's basic Call Protect service blocks scam calls but only flags spam.[31] Consumers who seek more comprehensive protections from a broad array of nuisance calls can select additional categories

[27] Declaratory Ruling, *supra* note 1.
[28] Letter from Joan Marsh, AT&T, to the Honorable Geoffrey Starks (June 10, 2019), https://docs.fcc.gov/public/attachments/DOC-358443A2.pdf.
[29] Commissioner Geoffrey Starks Releases Responses to His Inquiry Into the Availability of Free, Default Robocall Blocking Services (July 11, 2019), https://docs.fcc.gov/public/attachments/DOC-358443A1.pdf.
[30] 30 FCC Rcd 7961 (10) at ¶ 154.
[31] AT&T Call Protect (last visited July 21, 2019), https://www.att.com/features/security-apps.html.

of calls to block, for a monthly fee.[32] Clearly, phone companies have the ability to offer these services.

Personal blacklists

These call-blocking offerings should allow consumers to create their own individual blacklists, to more surgically stop any unwanted calls that have slipped through the carrier-level blocking and screening. (Whitelists will be discussed in more detail in the next section). AT&T's Call Protect likewise offers the capability to create personal blacklists.[33] All of these services should be offered at no additional line item charge, since consumers should not be forced to pay extra to deal with the flood of unwanted robocalls.

Safe harbor only for blocking spoofed calls deliberately circumventing SHAKEN/STIR.

The FCC has proposed a safe harbor to encourage carriers to block certain unverified calls. While our goal is to get to the point that all scam calls are stopped before they reach the consumer, at this point—before caller ID authentication is fully in place—the FCC should consider only a very narrow safe harbor, only for calls that phone companies have very high confidence are illegitimate. For example, a safe harbor should be provided for blocking calls in which someone not only tried to spoof the caller ID, but they tried to indicate that the information was verified.[34] It would not be appropriate to block calls solely on the basis that they are unauthenticated at this point, because SHAKEN/STIR is not currently viable for many calls. And this would hurt callers originating calls from those jurisdictions in with SHAKEN/STIR cannot yet be implemented.

The FCC should develop policies for improperly blocked calls that leave call recipients in control, including limiting a "critical calls" whitelist to authenticated, genuine emergency calls only, with a separate unblocking system, created by the FCC, guided by a specific set of criteria, and paid for by the members of the calling industry who seek to benefit from using it.

As call authentication strategies are adopted, there should be less fraudulent traffic entering the system, and blocking will have greater accuracy. Blocking mistakes must be minimal, and we expect that will be the case. However, the FCC should put in place procedures to guard against wanted calls being inappropriately intercepted. The FCC should also set up a system to ensure

[32] AT&T Call Protect FAQ (last visited July 21, 2019), https://www.att.com/features/security-apps.html#faqs.
[33] AT&T Call Protect, *supra* note 31.
[34] Fed. Commc'ns Comm'n, Advanced Methods to Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor, CG Docket No. 17-59, WC Docket No. 17-97 ¶ 3 (June 24, 2019), https://www.regulations.gov/document?D=FCC-2019-0188-0002.

that important and wanted calls get through, and that ensures consumer wishes are respected. Above all, the consumer must remain in control of what calls they receive.

Critical calls list for authenticated, genuine emergency calls and calls directly from government agencies only.

First, the FCC should set up a central "critical calls" list that gives specific numbers, like designated emergency numbers, an automatic green light. As noted in the NPRM, only authenticated calls should be whitelisted.[35] Otherwise scammers would be incentivized to spoof emergency numbers on a whitelist, making our current spoofing problem even worse.

The critical calls list should apply to genuine emergency calls and calls directly from government agencies only. Local telephone providers should be in control of listing these emergency numbers and other government numbers with the FCC, to ensure appropriate controls over inclusion. This critical calls list should not become a way for telemarketers to override consumer blocking preferences.

This list should include:

- All local and federal law enforcement (town, city, county, borough, state) telephone numbers used to investigate crimes and enforce the criminal law.
- All local government numbers used to make emergency calls regarding weather alerts, fire hazards, other physical threat to the health and safety of residents.
- Other calls from local, state, or federal government—not their agents—calling consumers for matters related to emergencies, and/or governmental benefits or services.

No private businesses should be on the critical calls list. Phone numbers used by local public schools to alert parents of school emergencies may be added to the generic white list. But calls from those numbers should be limited to real emergencies. Calls from schools that provide reminders of upcoming conferences, or band rehearsals, etc. should not be included on the critical calls list.

Individual consumer whitelists

To bridge the distinction between real government emergency calls and other automated calls that consumers want, as noted above, individual consumers should be able to generate their own whitelists with their providers to allow certain callers to be put through. Consumers should remain in control of their own personal whitelists, and be able to add and delete numbers at their discretion. Automated calls from private schools, even for emergencies, will have to be registered on consumers' individual white lists. Similarly, calls from banks, doctors, hospitals, and others that provide alerts or reminders should be handled through the personalized white

[35] *Id*. at ¶ 13.

lists. Once numbers are registered on consumers' whitelists, consumers should always have the ability to remove those numbers, and effectively block the calls. Additionally, if the consumer asks these callers to stop calling, the callers should be required to remove these numbers from their internal whitelists.

Call-unblocking system

Second, the FCC should establish a call-unblocking system, governed by a specified set of criteria. There should be a standard notification, established by the FCC, so that the caller knows that a call has been intercepted. Callers, particularly residential callers and those not engaging in high-volume traffic, should be informed when calls are blocked. For a call to be unblocked, its caller ID information must be authenticated, to ensure that scammers are not seeking to evade blocks. Evaluators should have a reasonable basis to believe that the call is not unlawful before unblocking it. Even so-called "legitimate" callers may make calls in violation of the consent requirements of the Telephone Consumer Protection Act (TCPA) or the Do Not Call Registry, and the caller's history of TCPA compliance should be considered before unblocking any of its calls.

Above all, consumer preferences should never be overridden. The call recipient must be consulted before a call to them is unblocked. Finally, the system must be paid for by callers who will benefit from its availability. The costs of controlling robocalls should not be borne by consumers. This is similar to the Do Not Call registry, which is paid for by callers seeking to consult the list.[36]

Conclusion

As stakeholders have long acknowledged, fully addressing the robocalls problem will be a multi-pronged effort. Consumers must have bedrock legal protections ensuring that they always have the ability to decide whether or not to receive a robocall. But technology has an important role to play as well in ensuring that scam and other unwanted calls are actually stopped before they reach the consumer. For too long, scammers and others have been able to hide behind caller ID spoofing in order to inundate consumers with unwanted and harmful calls without penalty. With the appropriate policies—including strong legal protections, holding phone companies and gateway providers accountable for knowing their customers, limiting the bad traffic before it enters the system, verifying caller ID information, and appropriate screening and other mitigation techniques to intercept other unwanted traffic—consumers will finally have meaningful control over the calls they receive. Please contact Maureen Mahoney, mmahoney@consumer.org, or Margot Saunders, msaunders@nclc.org, with any questions.

[36] Fed. Trade Comm'n, *National Do Not Call Registry, Information for Businesse*s (last visited July 21, 2019), https://www.donotcall.gov/faq/faqbusiness.aspx.

Respectfully submitted,

Maureen Mahoney
Policy Analyst
Consumer Reports

Margot Saunders
Senior Policy Counsel
National Consumer Law Center