May 21, 2026

Mr. John Stankey
Chairman & Chief Executive Officer
AT&T Inc.
Corporate Communications
208 S. Akard St.
Dallas, TX 75202

Mr. Stankey:

I write today to request information on AT&T Inc.'s efforts to prevent scammers from misusing its services. In recent years, global organized criminal networks have used a range of technologies to create increasingly convincing scams, which contribute to a booming scam economy that surpasses the global drug trade as an illicit industry.[1] Last year, for example, the FBI recorded over $20 billion in losses to scams and other cyber-enabled crimes.[2] As leaders of the Joint Economic Committee (JEC), we explored this important issue in a recent bipartisan hearing on *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, during which expert witnesses – including senior federal law enforcement officials – made clear that telecommunications companies have a front line role to play in this effort.[3] As one of the nation's largest cellular providers, AT&T has rightfully recognized that scams are a pervasive problem and that customers should have the ability to answer their calls and texts with confidence.[4] I hope that we can work together productively on this important issue.

---

[1] *Myanmar's Scam Empire Gets Worse, Not Better*, Economist (May 29, 2025) (www.economist.com/asia/2025/05/29/myanmars-scam-empire-gets-worse-not-better).

[2] FBI Internet Crime Complaint Center, *Internet Crime Report 2025* (www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf).

[3] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[4] AT&T, *What Is AT&T ActiveArmor℠ Mobile Security?* (www.att.com/wireless/what-is-activearmor-security/) (accessed Mar. 10, 2026).

Spam – a category of unwanted communications from nuisance telemarketers, illegal scammers, and others – can easily be sent to large numbers of people worldwide at little cost.[5] In 2024, wireless providers prevented a record 55 billion spam and scam robotexts from reaching customers, and they also block, label, or identify 45 billion scam calls annually, according to the statement that industry trade group CTIA submitted for our Committee hearing.[6] The number of unwanted messages that continue to reach customers is also staggering. According to YouMail, a robocall blocking company, Americans received nearly 52.5 billion robocalls in 2025 – an average of around 4.3 billion robocalls each month.[7] YouMail has further noted that "[o]ver the past five years, annual robocall volume has consistently remained between approximately 50 billion and 55 billion robocalls."[8] In 2024, Americans received an average of 19.2 billion spam texts each month – a more than threefold increase over 2020, according to RoboKiller, another spam-blocking company.[9] This high volume of spam traffic continues to contribute to mounting scam losses. Text messages and phone calls are the first and third most common methods that scammers use to initiate contact with victims, according to reports filed with the Federal Trade

---

[5] Federal Trade Commission, *Robocalls* (Sept. 2023) (consumer.ftc.gov/articles/robocalls); Federal Trade Commission, *National Do Not Call Registry FAQs* (consumer.ftc.gov/national-do-not-call-registry-faqs) (accessed Feb. 13, 2025); Federal Trade Commission, *How to Recognize and Report Spam Text Messages* (consumer.ftc.gov/articles/how-recognize-report-spam-text-messages#spam) (July 2022); PIRG, *Ringing in Your Fears 2025* (Oct. 2025) (publicinterestnetwork.org/wp-content/uploads/2025/10/RIOF-2025-REPORT-10151035.pdf); *Welcome to the Golden Age of Scams*, TIME (Sept. 18, 2024) (time.com/7021745/the-age-of-scams-2/); *Yes, It's Bad. Robocalls, and Their Scams, Are Surging,* New York Times (May 6, 2018) (www.nytimes.com/2018/05/06/your-money/robocalls-rise-illegal.html).

[6] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[7] *U.S. Consumers Received 52.5 Billion Robocalls in 2025, Over 4.1 Billion in December, According to YouMail Robocall Index*, YouMail (Jan. 8, 2026) (www.prnewswire.com/news-releases/us-consumers-received-52-5-billion-robocalls-in-2025--over-4-1-billion-in-december-according-to-youmail-robocall-index-302656174.html); YouMail Robocall Index, *Historical Robocalls by Time* (robocallindex.com/history/time) (accessed Feb. 13, 2026).

[8] *U.S. Consumers Received 52.5 Billion Robocalls in 2025, Over 4.1 Billion in December, According to YouMail Robocall Index*, YouMail (Jan. 8, 2026) (www.prnewswire.com/news-releases/us-consumers-received-52-5-billion-robocalls-in-2025--over-4-1-billion-in-december-according-to-youmail-robocall-index-302656174.html).

[9] PIRG, *Ringing in Your Fears 2025* (Oct. 2025) (publicinterestnetwork.org/wp-content/uploads/2025/10/RIOF-2025-REPORT-10151035.pdf); RoboKiller, *The Robocall Report 2021 Mid-Year Phone Scam Report* (2021) (cdn.prod.website-files.com/625442b4613eaa38d6514c11/62711527a014363ccfd3cd1e_robokiller_mid_year_phone_report.pdf).

Commission (FTC).[10] These scams are responsible for the highest median losses, with the FTC recording median losses of $1,835 for phone call-initiated scams and $1,000 for text-initiated scams per victim in 2025.[11]

Consumers need to be able to trust that the calls and texts they receive – from their doctor's office or their child's school, for example – are authentic. Scam communications, however, are increasingly difficult to distinguish from legitimate messages, and too much of the burden of detection is falling on customers.[12] Both the Federal Communications Commission (FCC) and AARP are so concerned about the safety and reliability of phone calls that they advise Americans to never answer calls from unknown numbers.[13] While this guidance may seem extreme, it may not actually go far enough, because the threat of phone scams extends beyond unknown callers. Kathy Stokes, director of the AARP's Fraud Prevention Programs, noted during the March hearing that it may be risky to answer *any* phone call, explaining that AARP had debated "whether we should call people picking up the telephone 'risky behavior.'"[14] In part, this is because "[s]cammers have successfully compromised caller ID," according to the *Washington Post*.[15] Using easily acquired spoofing technology, scammers can manipulate caller ID to make it appear as though they are calling from a local number, a real company, or another trusted source.[16] Once on the line, scammers can use AI voice technology to convincingly impersonate a bank employee, government official, or even a victim's loved one, for example.[17] Criminals will

---

[10] FTC, *Consumer Sentinel Network* (2025) (public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods).

[11] *Id.*

[12] Federal Communications Commission, *Stop Illegal Robocalls and Texts* (Feb. 27, 2026) (www.fcc.gov/sites/default/files/stop_unwanted_robocalls_and_texts.pdf); AARP, *Why You Shouldn't Answer Calls From Unknown Numbers* (July 8, 2024) (www.aarp.org/money/scams-fraud/unknown-number-do-not-answer/).

[13] Federal Communications Commission, *Stop Unwanted Robocalls and Texts* (Mar. 3, 2025) (www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts#:~:text=Don't%20answer%20calls%20from,being%20pressured%20for%20information%20immediately); AARP, *Why You Shouldn't Answer Calls From Unknown Numbers* (July 8, 2024) (www.aarp.org/money/scams-fraud/unknown-number-do-not-answer/).

[14] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[15] *Sick of Scams? Stop Answering Your Phone.*, Washington Post (June 17, 2024) (www.washingtonpost.com/technology/2024/06/17/phone-scams-dont-answer/).

[16] *Id.*

[17] Federal Trade Commission, *Scammers Use AI to Enhance Their Family Emergency Schemes* (Mar. 20, 2023) (consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes); *AI Phone Scam Mimicking Your Voice Can Now Be Used to*

often research their victims ahead of time, which they can do at scale with AI, so that their scams are highly personalized and therefore more believable.[18]

Importantly, wireless companies have taken steps to protect their customers, but they face significant challenges in defending against well-resourced, ever-evolving criminal scam operations that "continue to find new ways to reach consumers," according to the statement submitted for the JEC hearing by CTIA.[19] Companies, for example, have implemented branded calling – a paid service in which vetted companies can display their name, logo, and reason for calling on a recipient's device.[20] CTIA has called this technology "the next generation of call authentication" and claimed it was "already providing real results for millions of consumers."[21] Even some in other sectors agree that branded caller ID may be a potentially useful tool. In a joint comment submitted to the FCC in January 2026, multiple financial services industry trade associations called branded caller ID "a promising next step in the evolution of call authentication and the fight against illegal robocalls."[22]

Scam Family, Friends, Experts Warn, ABC7 (May 20, 2024) (abc7chicago.com/post/ai-phone-scam-calls-mimicking-voice-scam-family/14847406/); Federal Communications Commission, *Deep-Fake Audio and Video Links Make Robocalls and Scam Texts Harder to Spot* (June 8, 2024) (www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-scam-texts-harder-spot); *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert).

[18] *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert); *AI Phone Scam Mimicking Your Voice Can Now Be Used to Scam Family, Friends, Experts Warn*, ABC7 (May 20, 2024) (abc7chicago.com/post/ai-phone-scam-calls-mimicking-voice-scam-family/14847406/).

[19] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[20] *Id.*; CTIA, *Branded Calling ID™ Best Practices* (Nov. 2022) (api.ctia.org/wp-content/uploads/2022/11/Branded-Calling-Best-Practices.pdf).

[21] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[22] American Bankers Association et al., *Comments before the Federal Communications Commission in the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls et al.* (Jan. 5, 2026) (bpi.com/wp-content/uploads/2026/01/Joint-Trades-Urge-FCC-to-go-Further-on-Fraud-Prevention.pdf).

Still, consumer advocates, financial institutions, and other issue experts have called on telecommunications providers to take additional steps to authenticate users on their networks.[23] Hearing witness Reva Price, a Commissioner of the U.S.-China Economic and Security Review Commission and an expert on Southeast Asian scam compounds, testified during the JEC hearing that telecommunication carriers, along with social media platforms, should "implement stronger verification and detection measures."[24] Wireless providers have faced additional questions about the common industry practice of charging individual customers to access the strongest tools to protect against spam. The consumer advocacy organization PIRG, for example, has argued that "[n]o company should charge extra for essential protection services," adding, "[t]his isn't a luxury feature; it's a necessity."[25]

Our recent hearing also made clear that telecommunications companies need to take further steps to protect customers from scammers even as they serve as key partners on scams prevention for federal officials. JEC hearing witness Lois Greisman, associate director of the Division of Marketing Practices at the FTC, testified that the FTC works "very closely with the U.S. telecoms industry traceback group to identify phone scams that are coming in from abroad, hitting a gateway provider in the U.S., and to take action, whether through warning letters or law enforcement, to cut that access to the foreign networks."[26] At the same time, Richard Goldberg, associate counsel in the Fraud Section of the Department of Justice's Criminal Division, testified that telecommunications companies, along with social media and email providers, "need to continue to improve their systems to prevent victims from being reached in the first place."[27] Karen Seifert, director of the Scam Center Strike Force in the U.S. Attorney's Office for the District of Columbia, similarly argued that efforts by carriers to label suspicious phone calls are "a start, but the next step is to not even allow that phone call to come through."[28]

Expert witnesses, telecommunications providers, and other frontline industries agree that scams present an urgent and complex challenge that calls for additional action.[29] As leaders of

---

[23] *Id.*; PIRG, *Is Your Phone Company Protecting You from Scams?* (Mar. 27, 2025) (pirg.org/articles/is-your-phone-company-protecting-you-from-scams/).

[24] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[25] PIRG, *Is Your Phone Company Protecting You from Scams?* (Mar. 27, 2025) (pirg.org/articles/is-your-phone-company-protecting-you-from-scams/).

[26] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[27] *Id.*

[28] *Id.*

[29] Joint Economic Committee, Testimony Submitted for the Record on Behalf of the American Bankers Association, *The Rising Global Scam Economy: Modernizing Federal*

the Joint Economic Committee, we stand ready to work together on solutions to better protect Americans from scams. To help the Committee better understand AT&T's operations and efforts to prevent scams, I seek answers to the questions below.

The following questions pertain to steps AT&T has taken to protect its customers and wireless network in the United States. Unless otherwise specified, the applicable time period is 2021 through 2025, and this request pertains to all AT&T Inc.-branded entities that provide cellular telephone service in the United States. The term "communications" below refers to voice calls, including messages left on voicemail, as well as text messages, but it does not include third-party "over-the-top" messages or other messages that are received through services that AT&T does not provide directly.

1. Please describe AT&T's overall strategy for identifying and protecting its U.S. customers and network from illegal or unwanted spam and/or scam calls and texts.

    a. Please describe automated efforts and efforts which involve human review to identify illegal or unwanted spam and/or scam calls and texts, the factors AT&T uses for this identification, and the circumstances under which the company deploys these efforts.

    b. Please provide AT&T's approximate annual payroll costs, including salaries and other direct compensation to employees, consultants, independent contractors, and other workers in the U.S.
        i. What percentage of these costs are intended to protect the safety of AT&T's U.S. network and customers?
        ii. What percentage of these costs are attributable to work specifically to protect against scam communications?

    c. How much has AT&T invested per year in protecting against scam communications?

2. To the extent that AT&T attempts to identify scam attempts through calls and texts on its U.S. network:

    a. How many suspected illegal or unwanted spam and/or scam calls and texts targeting AT&T's U.S. network and customers has the company identified per year since 2021? For purposes of this question, "[s]pam is an unsolicited message sent to your mobile phone or email, often to promote goods and

---

Approaches to Protect Americans from Foreign Fraudsters, 119th Cong. (Mar. 25, 2026) (Joint Event 338091); Joint Economic Committee, Statement submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

services, push a political or social agenda or spread a virus," per AT&T's website.[30]

i. What percentage of overall call and text traffic on AT&T's U.S. network per year has been suspected illegal or unwanted spam and/or scam calls and texts? Of these messages, what percentage were suspected scam activity?
ii. How much revenue has suspected illegal or unwanted spam and/or scam calls and texts on AT&T's U.S. network generated for the company per year?
iii. What percentage of suspected illegal or unwanted spam and/or scam calls and texts per year has originated from parties outside the U.S.? Please provide a geographic breakdown of this activity for each year if available.
iv. What percentage of suspected illegal or unwanted spam and/or scam calls and texts on AT&T's U.S. network has AT&T blocked?

b. Roughly how many illegal or unwanted spam and/or scam calls and texts does AT&T identify via its internal detection tools, how many are reported by customers, and how many are reported to AT&T from other sources?
i. On average, approximately how many flagged communications from users or other outside sources are reported to AT&T daily?
ii. Please describe the steps that AT&T takes once it receives reports of spam and/or scam messages from users or other outside sources, including but not limited to customers who opt to report spam on their iPhones or Android phones.
iii. Of these flagged communications, how many calls and texts has AT&T identified as being spam and/or scam activity, and how does it make that determination? Please specify if such a determination requires human review.
iv. For each communication reported to AT&T, how long on average does it take AT&T to review and make a determination that these communications are or are not spam and/or scam activity?

c. Under what circumstances does AT&T alert customers that an incoming call or text is likely an illegal or unwanted spam and/or scam communication?

3. What actions does the company take when it identifies a phone number and/or account holder on the AT&T network that is responsible for sending illegal or unwanted spam and/or scam calls and texts?

[30] AT&T, Cyber Aware Spam Awareness & Education (about.att.com/pages/cyberaware/ae/spam) (accessed Mar. 17, 2026).

a. Does AT&T take steps to trace the caller/sender responsible? If so, does it work with additional parties to do so, such as the Industry Traceback Group and/or law enforcement?
    i. For AT&T customers responsible for such calls or texts, what, if any, know-your-customer information does AT&T collect that aids the company in identifying specific customers misusing its services?

b. Under what circumstances, and following what level of internal and/or external review, will AT&T suspend the account of a customer the company has determined to be responsible for sending illegal or unwanted spam and/or scam calls and texts? In your answer, please differentiate between customers who use your services for personal, household or family purposes, customers who use your services for business purposes, and reseller or wholesale customers.
    i. How many accounts has AT&T suspended per year for these reasons?
        1. How many accounts were subsequently reinstated?
        2. For accounts that were suspended and then reinstated, what is the average length of time the account was suspended?
    ii. What measures does AT&T undertake to ensure that individuals associated with these accounts and phone numbers do not attempt to create a new AT&T account or otherwise operate on the company's U.S. network?
    iii. How does AT&T implement phone number blocking? Please describe any do-not-originate and block lists that AT&T uses.

c. What efforts does AT&T undertake, if any, to determine whether accounts associated with illegal or unwanted spam and/or scam calls and texts have connections to a criminal network, a foreign government, sanctioned individuals or groups, or other individuals the U.S. has designated as threats, including Specially Designated Nationals?

d. Under what circumstances, if any, will AT&T contact law enforcement to report illegal activity on its networks, including evidence of scams?

e. Under what circumstances, if any, will AT&T report spam or illegal activity on its networks to entities that are not law enforcement, such as the FCC and CTIA's Secure Messaging Initiative?

4. Does AT&T share information with or seek information from other providers in the call path – which may include originating, terminating, gateway, and non-gateway intermediate providers, depending on the call – to help trace, track, and eliminate illegal or unwanted spam and/or scam calls and texts? Relatedly, does AT&T attempt to determine if such call providers have supported such communications, and what actions will AT&T take in response?

5. Does AT&T seek to determine if calls are made using AI-generated voices?

    a. If so, does the company alert customers when they receive a call that uses an AI-generated voice?

    b. If not, why not?

6. AT&T offers customers spam protection through its ActiveArmor service. The basic version of this service is available to customers for free, but the premium version requires an additional monthly fee.[31] Regarding this service:

    a. Please describe AT&T's reasoning for charging customers for the premium version of ActiveArmor instead of offering comprehensive protection from illegal or unwanted spam and/or scam calls to all customers by default.

    b. What percentage of AT&T customers with eligible devices use the free version of ActiveArmor, the premium version of ActiveArmor, and no version of ActiveArmor at all?
        i. What spam protections, if any, does AT&T provide for customers who do not use ActiveArmor?

    c. Please provide the total annual gross revenue generated by customers paying for the premium ActiveArmor service for each year since it was first introduced.

    d. Does ActiveArmor come pre-loaded on eligible devices? If so, please explain. If not, why not?

    e. Does AT&T track the number of customers subscribed to the premium version of ActiveArmor who do not use the additional features for which they are charged?
        i. If so, does AT&T alert premium customers when they are not using the additional ActiveArmor features?

    f. For customers who use the free version of ActiveArmor, use the premium version of ActiveArmor, and do not use ActiveArmor, respectively, how many illegal or unwanted spam and/or scam texts and calls has AT&T alerted customers to each year since 2021, and how many of these texts and calls has AT&T blocked?

[31] AT&T, *What is ActiveArmor Mobile Security* (www.att.com/wireless/what-is-activearmor-security/) (accessed Mar.10, 2026).

g. How many customer reports of illegal or unwanted spam and/or scam calls and texts has AT&T received through ActiveArmor each year since it launched? How many unique phone numbers have been reported each year?

7. Is AT&T able to track how many illegal or unwanted spam and/or scam calls and texts evaded detection from its spam filters – for instance, as part of an audit of security measures? If not, why not? If so:

    a. For each year since 2021, how many unlabeled, likely illegal or unwanted spam and/or scam calls and texts reached AT&T customers who use the free version of the ActiveArmor app, use the premium version of the ActiveArmor app, and do not use the ActiveArmor app, respectively?

8. Please detail AT&T's policies and procedures with respect to customers, including businesses and charities, that send a high volume of phone calls and/or text messages. How does AT&T ensure that these customers send bulk communications only to those who have consented to receiving such messages?

9. Does AT&T limit the number of calls a wireless subscriber line can place in a single day or other interval of time?

    a. Does AT&T monitor the volume of calls placed by a wireless subscriber line as an indicator that the line is being used in a SIM farm?[32]

    b. What actions does AT&T take if it suspects a wireless subscriber line is being used in a SIM farm?

10. Please detail AT&T's policies and procedures with respect to spoofed calls, in which a caller intentionally falsifies caller ID. Specifically:

    a. What steps does AT&T take to determine that spoofed calls are legitimate (such as a spoofed number from a doctor's office)? Does AT&T specifically monitor for spoofed calls originating from abroad that present as U.S. phone numbers? If not, why not? If so, what is AT&T's success rate for identifying such calls, and what action does the company take when it detects these calls?

---

[32] According to PBS, "SIM farms are hardware devices that can hold numerous SIM cards from different mobile operators. These devices then exploit voice over internet protocol (VoIP) technology to send and receive bulk messages or calls. While initially developed for legitimate purposes, such as low cost international calling, the technology has become a cornerstone of organized fraud targeting mass audiences — phishing texts and scam calls." *How 'SIM Farms' Like the One Found Near the UN Could Collapse Telecom Networks,* PBS (Sept. 23, 2025) (www.pbs.org/newshour/nation/how-sim-farms-like-the-one-found-near-the-un-could-collapse-telecom-networks).

b. Does AT&T specifically monitor for spoofed caller IDs that misrepresent callers as an existing entity, such as a bank or federal agency? If not, why not? If so, what action does it take when it detects these calls?

11. In 2025, AT&T ended its email-to-text and text-to-email feature – a service that is often abused by scammers.[33] What factors led AT&T to disable email-to-text and text-to-email capabilities?

    a. Specifically, did AT&T detect spammers and/or scammers misusing email-to-text and text-to-email services on its network? If so, did that contribute to the company's decision to halt this service? Please explain.

12. In 2024, AT&T announced it was launching Branded Call Display on its network.[34]

    a. What company/companies does AT&T contract with to deliver branded calls?

    b. How does AT&T, or any company it contracts with to deliver branded calls, vet companies seeking to send branded calls on its network?

    c. If AT&T has reason to believe that a branded call on its network is illegitimate, what steps does it take?

    d. How much does AT&T charge businesses to place branded and un-branded calls, respectively, on AT&T's network?

Please provide your responses as soon as possible but in no event later than June 11, 2026. If you have any questions related to this request, please contact [redacted]

Sincerely,

---

[33] AT&T, *Say Goodbye To Email-To-Text And Text-To-Email* (www.att.com/support/article/wireless/KM1061254/) (accessed Mar. 16, 2026); Herb Weisbaum, *Cybercriminals Use Email to Text Scams: How They Evade Spam Filters and What You Can Do*, KOMO News (Sept. 30, 2023) (komonews.com/news/consumer/why-am-i-getting-emails-messages-in-my-text-folder-scams-cyber-crime-cybercriminals-consumers-aarp-fraud-prevention-network-spammers).

[34] Transunion, *AT&T and TransUnion Launch the Industry's First In-Network Branded Call Display with Logos* (Jan. 30, 2024) (newsroom.transunion.com/att-and-transunion-launch-the-industrys-first-in-network-branded-call-display-with-logos/).

David Schweikert
Chairman

Margaret Wood Hassan
Ranking Member

cc: Eric Schmitt
Vice Chairman, Joint Economic Committee

May 21, 2026

Mr. Srini Gopalan
President & Chief Executive Officer
T-Mobile USA, Inc.
12920 SE 38th Street
Bellevue, Washington 98006

Mr. Gopalan:

I write today to request information on T-Mobile's efforts to prevent scammers from misusing its services. In recent years, global organized criminal networks have used a range of technologies to create increasingly convincing scams, which contribute to a booming scam economy that surpasses the global drug trade as an illicit industry.[1] Last year, for example, the FBI recorded over $20 billion in losses to scams and other cyber-enabled crimes.[2] As leaders of the Joint Economic Committee (JEC), we explored this important issue in a recent bipartisan hearing on *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, during which expert witnesses – including senior federal law enforcement officials – made clear that telecommunications companies have a front line role to play in this effort.[3] As one of the nation's largest cellular providers, T-Mobile has rightfully recognized that scams are a pervasive problem and that customers should have the ability to answer their calls and texts with confidence.[4] I hope that we can work together productively on this important issue.

---

[1] *Myanmar's Scam Empire Gets Worse, Not Better*, Economist (May 29, 2025) (www.economist.com/asia/2025/05/29/myanmars-scam-empire-gets-worse-not-better).

[2] FBI Internet Crime Complaint Center, *Internet Crime Report 2025* (www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf).

[3] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[4] T-Mobile, *Put a Stop to Scam Calls with Scam Shield.* (www.t-mobile.com/benefits/scam-shield) (accessed Mar. 16, 2026).

Spam – a category of unwanted communications from nuisance telemarketers, illegal scammers, and others – can easily be sent to large numbers of people worldwide at little cost.[5] In 2024, wireless providers prevented a record 55 billion spam and scam robotexts from reaching customers, and they also block, label, or identify 45 billion scam calls annually, according to the statement that industry trade group CTIA submitted for our Committee hearing.[6] The number of unwanted messages that continue to reach customers is also staggering. According to YouMail, a robocall blocking company, Americans received nearly 52.5 billion robocalls in 2025 – an average of around 4.3 billion robocalls each month.[7] YouMail has further noted that "[o]ver the past five years, annual robocall volume has consistently remained between approximately 50 billion and 55 billion robocalls."[8] In 2024, Americans received an average of 19.2 billion spam texts each month – a more than threefold increase over 2020, according to RoboKiller, another spam-blocking company.[9] This high volume of spam traffic continues to contribute to mounting scam losses. Text messages and phone calls are the first and third most common methods that scammers use to initiate contact with victims, according to reports filed with the Federal Trade

---

[5] Federal Trade Commission, *Robocalls* (Sept. 2023) (consumer.ftc.gov/articles/robocalls); Federal Trade Commission, *National Do Not Call Registry FAQs* (consumer.ftc.gov/national-do-not-call-registry-faqs) (accessed Feb. 13, 2025); Federal Trade Commission, *How to Recognize and Report Spam Text Messages* (consumer.ftc.gov/articles/how-recognize-report-spam-text-messages#spam) (July 2022); PIRG, *Ringing in Your Fears 2025* (Oct. 2025) (publicinterestnetwork.org/wp-content/uploads/2025/10/RIOF-2025-REPORT-10151035.pdf); *Welcome to the Golden Age of Scams*, TIME (Sept. 18, 2024) (time.com/7021745/the-age-of-scams-2/); *Yes, It's Bad. Robocalls, and Their Scams, Are Surging,* New York Times (May 6, 2018) (www.nytimes.com/2018/05/06/your-money/robocalls-rise-illegal.html).

[6] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[7] *U.S. Consumers Received 52.5 Billion Robocalls in 2025, Over 4.1 Billion in December, According to YouMail Robocall Index*, YouMail (Jan. 8, 2026) (www.prnewswire.com/news-releases/us-consumers-received-52-5-billion-robocalls-in-2025--over-4-1-billion-in-december-according-to-youmail-robocall-index-302656174.html); YouMail Robocall Index, *Historical Robocalls by Time* (robocallindex.com/history/time) (accessed Feb. 13, 2026).

[8] *U.S. Consumers Received 52.5 Billion Robocalls in 2025, Over 4.1 Billion in December, According to YouMail Robocall Index*, YouMail (Jan. 8, 2026) (www.prnewswire.com/news-releases/us-consumers-received-52-5-billion-robocalls-in-2025--over-4-1-billion-in-december-according-to-youmail-robocall-index-302656174.html).

[9] PIRG, *Ringing in Your Fears 2025* (Oct. 2025) (publicinterestnetwork.org/wp-content/uploads/2025/10/RIOF-2025-REPORT-10151035.pdf); RoboKiller, *The Robocall Report 2021 Mid-Year Phone Scam Report* (2021) (cdn.prod.website-files.com/625442b4613eaa38d6514c11/62711527a014363ccfd3cd1e_robokiller_mid_year_phone_report.pdf).

Commission (FTC).[10] These scams are responsible for the highest median losses, with the FTC recording median losses of $1,835 for phone call-initiated scams and $1,000 for text-initiated scams per victim in 2025.[11]

Consumers need to be able to trust that the calls and texts they receive – from their doctor's office or their child's school, for example – are authentic. Scam communications, however, are increasingly difficult to distinguish from legitimate messages, and too much of the burden of detection is falling on customers. Both the Federal Communications Commission (FCC) and AARP are so concerned about the safety and reliability of phone calls that they advise Americans to never answer calls from unknown numbers.[12] While this guidance may seem extreme, it may not actually go far enough, because the threat of phone scams extends beyond unknown callers. Kathy Stokes, director of the AARP's Fraud Prevention Programs, noted during the March hearing that it may be risky to answer *any* phone call, explaining that AARP had debated "whether we should call people picking up the telephone 'risky behavior.'"[13] In part, this is because "[s]cammers have successfully compromised caller ID," according to the *Washington Post*.[14] Using easily acquired spoofing technology, scammers can manipulate caller ID to make it appear as though they are calling from a local number, a real company, or another trusted source.[15] Once on the line, scammers can use AI voice technology to convincingly impersonate a bank employee, government official, or even a victim's loved one, for example.[16] Criminals will

---

[10] FTC, *Consumer Sentinel Network* (2025) (public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods).

[11] *Id.*

[12] Federal Communications Commission, *Stop Unwanted Robocalls and Texts* (Mar. 3, 2025) (www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts#:~:text=Don't%20answer%20calls%20from,being%20pressured%20for%20information%20immediately); AARP, *Why You Shouldn't Answer Calls From Unknown Numbers* (July 8, 2024) (www.aarp.org/money/scams-fraud/unknown-number-do-not-answer/).

[13] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[14] *Sick of Scams? Stop Answering Your Phone.*, Washington Post (June 17, 2024) (www.washingtonpost.com/technology/2024/06/17/phone-scams-dont-answer/).

[15] *Id.*

[16] Federal Trade Commission, *Scammers Use AI to Enhance Their Family Emergency Schemes* (Mar. 20, 2023) (consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes); *AI Phone Scam Mimicking Your Voice Can Now Be Used to Scam Family, Friends, Experts Warn*, ABC7 (May 20, 2024) (abc7chicago.com/post/ai-phone-scam-calls-mimicking-voice-scam-family/14847406/); Federal Communications Commission, *Deep-Fake Audio and Video Links Make Robocalls and Scam Texts Harder to Spot* (June 8, 2024) (www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-

often research their victims ahead of time, which they can do at scale with AI, so that their scams are highly personalized and therefore more believable.[17]

Importantly, wireless companies have taken steps to protect their customers, but they face significant challenges in defending against well-resourced, ever-evolving criminal scam operations that "continue to find new ways to reach consumers," according to the statement submitted for the JEC hearing by CTIA.[18] Companies, for example, have implemented branded calling – a paid service in which vetted companies can display their name, logo, and reason for calling on a recipient's device.[19] CTIA has called this technology "the next generation of call authentication" and claimed it was "already providing real results for millions of consumers."[20] Even some in other sectors agree that branded caller ID may be a potentially useful tool. In a joint comment submitted to the FCC in January 2026, multiple financial services industry trade associations called branded caller ID "a promising next step in the evolution of call authentication and the fight against illegal robocalls."[21]

---

scam-texts-harder-spot); *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert).

[17] *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert); *AI Phone Scam Mimicking Your Voice Can Now Be Used to Scam Family, Friends, Experts Warn*, ABC7 (May 20, 2024) (abc7chicago.com/post/ai-phone-scam-calls-mimicking-voice-scam-family/14847406/).

[18] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[19] CTIA, *Branded Calling ID™ Best Practices* (Nov. 2022) (api.ctia.org/wp-content/uploads/2022/11/Branded-Calling-Best-Practices.pdf); Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[20] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[21] American Bankers Association et al., *Comments before the Federal Communications Commission in the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls et al.* (Jan. 5, 2026) (bpi.com/wp-content/uploads/2026/01/Joint-Trades-Urge-FCC-to-go-Further-on-Fraud-Prevention.pdf).

Still, consumer advocates, financial institutions, and other issue experts have called on telecommunications providers to take additional steps to authenticate users on their networks.[22] Hearing witness Reva Price, a Commissioner of the U.S.-China Economic and Security Review Commission and an expert on Southeast Asian scam compounds, testified during the JEC hearing that telecommunication carriers, along with social media platforms, should "implement stronger verification and detection measures."[23] Wireless providers have faced additional questions about the common industry practice of charging individual customers to access the strongest tools to protect against spam. The consumer advocacy organization PIRG, for example, has argued that "[n]o company should charge extra for essential protection services," adding, "[t]his isn't a luxury feature; it's a necessity."[24]

Our recent hearing also made clear that telecommunications companies need to take further steps to protect customers from scammers even as they serve as key partners on scams prevention for federal officials. JEC hearing witness Lois Greisman, associate director of the Division of Marketing Practices at the FTC, testified that the FTC works "very closely with the U.S. telecoms industry traceback group to identify phone scams that are coming in from abroad, hitting a gateway provider in the U.S., and to take action, whether through warning letters or law enforcement, to cut that access to the foreign networks."[25] At the same time, Richard Goldberg, associate counsel in the Fraud Section of the Department of Justice's Criminal Division, testified that telecommunications companies, along with social media and email providers, "need to continue to improve their systems to prevent victims from being reached in the first place."[26] Karen Seifert, director of the Scam Center Strike Force in the U.S. Attorney's Office for the District of Columbia, similarly argued that efforts by carriers to label suspicious phone calls are "a start, but the next step is to not even allow that phone call to come through."[27]

---

[22] American Bankers Association et al., *Comments Before the Federal Communications Commission in the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls et al.* (Jan. 5, 2026) (bpi.com/wp-content/uploads/2026/01/Joint-Trades-Urge-FCC-to-go-Further-on-Fraud-Prevention.pdf); PIRG, *Is Your Phone Company Protecting You from Scams?* (Mar. 27, 2025) (pirg.org/articles/is-your-phone-company-protecting-you-from-scams/).

[23] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[24] PIRG, *Is Your Phone Company Protecting You from Scams?* (Mar. 27, 2025) (pirg.org/articles/is-your-phone-company-protecting-you-from-scams/).

[25] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[26] *Id.*

[27] *Id.*

Expert witnesses, telecommunications providers, and other frontline industries agree that scams present an urgent and complex challenge that calls for additional action.[28] As leaders of the Joint Economic Committee, we stand ready to work together on solutions to better protect Americans from scams. To help the Committee better understand T-Mobile's operations and efforts to prevent scams, I seek answers to the questions below.

The following questions pertain to steps T-Mobile has taken to protect its customers and wireless network in the United States. Unless otherwise specified, the applicable time period is 2021 through 2025, and this request pertains to all T-Mobile-branded entities that provide cellular telephone service in the United States. The term "communications" below refers to voice calls, including messages left on voicemail, as well as text messages, but it does not include third-party "over-the-top" messages or other messages that are received through services that T-Mobile does not provide directly.

1. Please describe T-Mobile's overall strategy for identifying and protecting its U.S. customers and network from illegal or unwanted spam and/or scam calls and texts.

    a. Please describe automated efforts and efforts which involve human review to identify illegal or unwanted spam and/or scam calls and texts, the factors T-Mobile uses for this identification, and the circumstances under which the company deploys these efforts.

    b. Please provide T-Mobile's approximate annual payroll costs, including salaries and other direct compensation to employees, consultants, independent contractors, and other workers in the U.S.
        i. What percentage of these costs are intended to protect the safety of T-Mobile's U.S. network and customers?
        ii. What percentage of these costs are attributable to work specifically to protect against scam communications?

    c. How much has T-Mobile invested per year in protecting against scam communications?

2. To the extent that T-Mobile attempts to identify scam attempts through calls and texts on its U.S. network:

[28] Joint Economic Committee, Testimony Submitted for the Record on Behalf of the American Bankers Association, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091); Joint Economic Committee, Statement submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

a. How many suspected illegal or unwanted spam and/or scam calls and texts targeting T-Mobile's U.S. network and customers has the company identified per year since 2021? For purposes of this question, "Potential Spam calls are unwanted solicitation calls from numbers that aren't specifically intended for you. These differ from Scam Likely calls, which are usually fraudulent, illegal, and intended to harm you," as described on T-Mobile's website.[29]
    i. What percentage of overall call and text traffic on T-Mobile's U.S. network per year has been suspected illegal or unwanted spam and/or scam calls and texts? Of these messages, what percentage were suspected scam activity?
    ii. How much revenue has suspected illegal or unwanted spam and/or scam calls and texts on T-Mobile's U.S. network generated for the company per year?
    iii. What percentage of suspected illegal or unwanted spam and/or scam calls and texts per year has originated from parties outside the U.S.? Please provide a geographic breakdown of this activity for each year if available.
    iv. What percentage of suspected illegal or unwanted spam and/or scam calls and texts on T-Mobile's U.S. network has T-Mobile blocked?

b. Roughly how many illegal or unwanted spam and/or scam calls and texts does T-Mobile identify via its internal detection tools, how many are reported by customers, and how many are reported to T-Mobile from other sources?
    i. On average, approximately how many flagged communications from users or other outside sources are reported to T-Mobile daily?
    ii. Please describe the steps that T-Mobile takes once it receives reports of spam and/or scam messages from users or other outside sources, including but not limited to customers who opt to report spam on their iPhones or Android phones.
    iii. Of these flagged communications, how many calls and texts has T-Mobile identified as being spam and/or scam activity, and how does it make that determination? Please specify if such a determination requires human review.
    iv. For each communication reported to T-Mobile, how long on average does it take T-Mobile to review and make a determination that these communications are or are not spam and/or scam activity?

c. Under what circumstances does T-Mobile alert customers that an incoming call or text is likely an illegal or unwanted spam and/or scam communication?

[29] T-Mobile, *Put a Stop to Scam Calls with Scam Shield.* (www.t-mobile.com/benefits/scam-shield) (accessed Mar. 16, 2026).

3. What actions does the company take when it identifies a phone number and/or account holder on the T-Mobile network that is responsible for sending illegal or unwanted spam and/or scam calls and texts?

    a. Does T-Mobile take steps to trace the caller/sender responsible? If so, does it work with additional parties to do so, such as the Industry Traceback Group and/or law enforcement?
        i. For T-Mobile customers responsible for such calls or texts, what, if any, know-your-customer information does T-Mobile collect that aids the company in identifying specific customers misusing its services?

    b. Under what circumstances, and following what level of internal and/or external review, will T-Mobile suspend the account of a customer the company has determined to be responsible for sending illegal or unwanted spam and/or scam calls and texts? In your answer, please differentiate between customers who use your services for personal, household or family purposes, customers who use your services for business purposes, and reseller or wholesale customers.
        i. How many accounts has T-Mobile suspended per year for these reasons?
            1. How many accounts were subsequently reinstated?
            2. For accounts that were suspended and then reinstated, what is the average length of time the account was suspended?
        ii. What measures does T-Mobile undertake to ensure that individuals associated with these accounts and phone numbers do not attempt to create a new T-Mobile account or otherwise operate on the company's U.S. network?
        iii. How does T-Mobile implement phone number blocking? Please describe any do-not-originate and block lists that T-Mobile uses.

    c. What efforts does T-Mobile undertake, if any, to determine whether accounts associated with illegal or unwanted spam and/or scam calls and texts have connections to a criminal network, a foreign government, sanctioned individuals or groups, or other individuals the U.S. has designated as threats, including Specially Designated Nationals?

    d. Under what circumstances, if any, will T-Mobile contact law enforcement to report illegal activity on its networks, including evidence of scams?

    e. Under what circumstances, if any, will T-Mobile report spam or illegal activity on its networks to entities that are not law enforcement, such as the FCC and CTIA's Secure Messaging Initiative?

4. Does T-Mobile share information with or seek information from other providers in the call path – which may include originating, terminating, gateway, and non-gateway

intermediate providers, depending on the call – to help trace, track, and eliminate illegal or unwanted spam and/or scam calls and texts? Relatedly, does T-Mobile attempt to determine if such call providers have supported such communications, and what actions will T-Mobile take in response?

5. Does T-Mobile seek to determine if calls are made using AI-generated voices?

    a. If so, does the company alert customers when they receive a call that uses an AI-generated voice?

    b. If not, why not?

6. T-Mobile offers customers spam protection through its Scam Shield service.[30] The basic version of this service is available to customers for free, but the premium version requires an additional monthly fee.[31] Regarding this service:

    a. Please describe T-Mobile's reasoning for charging customers for the premium version of Scam Shield instead of offering comprehensive protection from illegal or unwanted spam and/or scam calls to all customers by default.

    b. What percentage of T-Mobile customers with eligible devices use the free version of Scam Shield, the premium version of Scam Shield, and no version of Scam Shield at all?
        i. What spam protections, if any, does T-Mobile provide for customers who do not use Scam Shield?

    c. Please provide the total annual gross revenue generated by customers paying for the premium Scam Shield service for each year since it was first introduced.

    d. Does Scam Shield come pre-loaded on eligible devices? If so, please explain. If not, why not?

    e. Does T-Mobile track the number of customers subscribed to the premium version of Scam Shield who do not use the additional features for which they are charged?
        i. If so, does T-Mobile alert premium customers when they are not using the additional Scam Shield features?

    f. For customers who use the free version of Scam Shield, use the premium version of Scam Shield, and do not use Scam Shield, respectively, how many

[30] *Id.*

[31] *Id.*

illegal or unwanted spam and/or scam texts and calls has T-Mobile alerted customers to each year since 2021, and how many of these texts and calls has T-Mobile blocked?

g. How many customer reports of illegal or unwanted spam and/or scam calls and texts has T-Mobile received through Scam Shield each year since it launched? How many unique phone numbers have been reported each year?

7. Is T-Mobile able to track how many illegal or unwanted spam and/or scam calls and texts evaded detection from its spam filters – for instance, as part of an audit of security measures? If not, why not? If so:

   a. For each year since 2021, how many unlabeled, likely illegal or unwanted spam and/or scam calls and texts reached T-Mobile customers who use the free version of Scam Shield, use the premium version of Scam Shield, and do not use Scam Shield, respectively?

8. Please detail T-Mobile's policies and procedures with respect to customers, including businesses and charities, that send a high volume of phone calls and/or text messages. How does T-Mobile ensure that these customers send bulk communications only to those who have consented to receiving such messages?

9. Does T-Mobile limit the number of calls a wireless subscriber line can place in a single day or other interval of time?

   a. Does T-Mobile monitor the volume of calls placed by a wireless subscriber line as an indicator that the line is being used in a SIM farm?[32]

   b. What actions does T-Mobile take if it suspects a wireless subscriber line is being used in a SIM farm?

10. Please detail T-Mobile's policies and procedures with respect to spoofed calls, in which a caller intentionally falsifies caller ID. Specifically:

    a. What steps does T-Mobile take to determine the legitimacy of a spoofed call (such as a doctor's office versus a scammer)? Does T-Mobile specifically

[32] According to PBS, "SIM farms are hardware devices that can hold numerous SIM cards from different mobile operators. These devices then exploit voice over internet protocol (VoIP) technology to send and receive bulk messages or calls. While initially developed for legitimate purposes, such as low cost international calling, the technology has become a cornerstone of organized fraud targeting mass audiences — phishing texts and scam calls." *How 'SIM Farms' Like the One Found Near the UN Could Collapse Telecom Networks,* PBS (Sept. 23, 2025) (www.pbs.org/newshour/nation/how-sim-farms-like-the-one-found-near-the-un-could-collapse-telecom-networks).

monitor for spoofed calls originating from abroad that present as U.S. phone numbers? If not, why not? If so, what is T-Mobile's success rate for identifying such calls, and what action does the company take when it detects these calls?

b. Does T-Mobile specifically monitor for spoofed caller IDs that misrepresent callers as an existing entity, such as a bank or federal agency? If not, why not? If so, what action does it take when it detects these calls?

11. T-Mobile describes email-to-text messaging – a feature that can easily be abused by scammers – as a "legacy system that may eventually be decommissioned in the future" on the company's networks.[33] The company limits this service to "consumer messaging" – which are messages exchanged between individual users – while prohibiting it for all non-consumer messages, which include account notifications from businesses and messages from high-volume senders, for example.[34]

    a. What factors led T-Mobile to limit its e-mail to text messaging service to certain customers?
        i. Specifically, has T-Mobile detected spammers and/or scammers misusing this service on its network? If so, did this factor into the company's decision to limit this service? Please explain.
        ii. Does T-Mobile intend to decommission this service entirely? Please explain.

12. In 2022, T-Mobile announced it was launching branded caller ID on its network.[35]

    a. What company/companies does T-Mobile contract with to deliver branded calls?

---

[33] T-Mobile, *Consumer Versus Non-Consumer Text Messaging* (www.t-mobile.com/support/plans-features/consumer-versus-non-consumer-text-messaging) (accessed Mar. 16, 2026); Herb Weisbaum**,** *Cybercriminals Use Email to Text Scams: How They Evade Spam Filters and What You Can Do*, KOMO News (Sept. 30, 2023) (komonews.com/news/consumer/why-am-i-getting-emails-messages-in-my-text-folder-scams-cyber-crime-cybercriminals-consumers-aarp-fraud-prevention-network-spammers).

[34] T-Mobile, *Consumer Versus Non-Consumer Text Messaging* (www.t-mobile.com/support/plans-features/consumer-versus-non-consumer-text-messaging) (accessed Mar. 16, 2026).

[35] T-Mobile, *T-Mobile Partners with CTIA to Implement Branded Caller ID Best Practices* (Jan. 18, 2022) (www.t-mobile.com/news/devices/t-mobile-partners-with-ctia-to-implement-branded-caller-id-best-practices).

b. How does T-Mobile, or any company it contracts with to deliver branded calls, vet companies seeking to send branded calls on its network?

c. If T-Mobile has reason to believe that a branded call on its network is illegitimate, what steps does it take?

d. How much does T-Mobile charge businesses to place branded and un-branded calls, respectively, on T-Mobile's network?

Please provide your responses as soon as possible but in no event later than June 11, 2026. If you have any questions related to this request, please contact [redacted]

Sincerely,

David Schweikert
Chairman

Margaret Wood Hassan
Ranking Member

cc: Eric Schmitt
Vice Chairman, Joint Economic Committee

May 21, 2026

Mr. Dan Schulman
Chief Executive Officer
Verizon
1095 Avenue of the Americas
New York, NY 10036

Mr. Schulman:

I write today to request information on Verizon's efforts to prevent scammers from misusing its services. In recent years, global organized criminal networks have used a range of technologies to create increasingly convincing scams, which contribute to a booming scam economy that surpasses the global drug trade as an illicit industry.[1] Last year, for example, the FBI recorded over $20 billion in losses to scams and other cyber-enabled crimes.[2] As leaders of the Joint Economic Committee (JEC), we explored this important issue in a recent bipartisan hearing on *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, during which expert witnesses – including senior federal law enforcement officials – made clear that telecommunications companies have a front line role to play in this effort.[3] As one of the nation's largest cellular providers, Verizon has rightfully recognized that scams are a pervasive problem and that customers should have the ability to answer their calls and texts with confidence.[4] I hope that we can work together productively on this important issue.

---

[1] *Myanmar's Scam Empire Gets Worse, Not Better*, Economist (May 29, 2025) (www.economist.com/asia/2025/05/29/myanmars-scam-empire-gets-worse-not-better).

[2] FBI Internet Crime Complaint Center, *Internet Crime Report 2025* (www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf).

[3] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[4] Verizon, *Call Filter* (www.verizon.com/solutions-and-services/add-ons/protection-and-security/call-filter/) (accessed Jan. 5, 2026).

Spam – a category of unwanted communications from nuisance telemarketers, illegal scammers, and others – can easily be sent to large numbers of people worldwide at little cost.[5] In 2024, wireless providers prevented a record 55 billion spam and scam robotexts from reaching customers, and they also block, label, or identify 45 billion scam calls annually, according to the statement that industry trade group CTIA submitted for our Committee hearing.[6] The number of unwanted messages that continue to reach customers is also staggering. According to YouMail, a robocall blocking company, Americans received nearly 52.5 billion robocalls in 2025 – an average of around 4.3 billion robocalls each month.[7] YouMail has further noted that "[o]ver the past five years, annual robocall volume has consistently remained between approximately 50 billion and 55 billion robocalls."[8] In 2024, Americans received an average of 19.2 billion spam texts each month – a more than threefold increase over 2020, according to RoboKiller, another spam-blocking company.[9] This high volume of spam traffic continues to contribute to mounting scam losses. Text messages and phone calls are the first and third most common methods that scammers use to initiate contact with victims, according to reports filed with the Federal Trade

[5] Federal Trade Commission, *Robocalls* (Sept. 2023) (consumer.ftc.gov/articles/robocalls); Federal Trade Commission, *National Do Not Call Registry FAQs* (consumer.ftc.gov/national-do-not-call-registry-faqs) (accessed Feb. 13, 2025); Federal Trade Commission, *How to Recognize and Report Spam Text Messages* (consumer.ftc.gov/articles/how-recognize-report-spam-text-messages#spam) (July 2022); PIRG, *Ringing in Your Fears 2025* (Oct. 2025) (publicinterestnetwork.org/wp-content/uploads/2025/10/RIOF-2025-REPORT-10151035.pdf); *Welcome to the Golden Age of Scams*, TIME (Sept. 18, 2024) (time.com/7021745/the-age-of-scams-2/); *Yes, It's Bad. Robocalls, and Their Scams, Are Surging,* New York Times (May 6, 2018) (www.nytimes.com/2018/05/06/your-money/robocalls-rise-illegal.html).

[6] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[7] *U.S. Consumers Received 52.5 Billion Robocalls in 2025, Over 4.1 Billion in December, According to YouMail Robocall Index*, YouMail (Jan. 8, 2026) (www.prnewswire.com/news-releases/us-consumers-received-52-5-billion-robocalls-in-2025--over-4-1-billion-in-december-according-to-youmail-robocall-index-302656174.html); YouMail Robocall Index, *Historical Robocalls by Time* (robocallindex.com/history/time) (accessed Feb. 13, 2026).

[8] *U.S. Consumers Received 52.5 Billion Robocalls in 2025, Over 4.1 Billion in December, According to YouMail Robocall Index*, YouMail (Jan. 8, 2026) (www.prnewswire.com/news-releases/us-consumers-received-52-5-billion-robocalls-in-2025--over-4-1-billion-in-december-according-to-youmail-robocall-index-302656174.html).

[9] PIRG, *Ringing in Your Fears 2025* (Oct. 2025) (publicinterestnetwork.org/wp-content/uploads/2025/10/RIOF-2025-REPORT-10151035.pdf); RoboKiller, *The Robocall Report 2021 Mid-Year Phone Scam Report* (2021) (cdn.prod.website-files.com/625442b4613eaa38d6514c11/62711527a014363ccfd3cd1e_robokiller_mid_year_phone_report.pdf).

Commission (FTC).[10] These scams are responsible for the highest median losses, with the FTC recording median losses of $1,835 for phone call-initiated scams and $1,000 for text-initiated scams per victim in 2025.[11]

Consumers need to be able to trust that the calls and texts they receive – from their doctor's office or their child's school, for example – are authentic. Scam communications, however, are increasingly difficult to distinguish from legitimate messages, and too much of the burden of detection is falling on customers.[12] Both the Federal Communications Commission (FCC) and AARP are so concerned about the safety and reliability of phone calls that they advise Americans to never answer calls from unknown numbers.[13] While this guidance may seem extreme, it may not actually go far enough, because the threat of phone scams extends beyond unknown callers. Kathy Stokes, director of the AARP's Fraud Prevention Programs, noted during the March hearing that it may be risky to answer *any* phone call, explaining that AARP had debated "whether we should call people picking up the telephone 'risky behavior.'"[14] In part, this is because "[s]cammers have successfully compromised caller ID," according to the *Washington Post*.[15] Using easily acquired spoofing technology, scammers can manipulate caller ID to make it appear as though they are calling from a local number, a real company, or another trusted source.[16] Once on the line, scammers can use AI voice technology to convincingly impersonate a bank employee, government official, or even a victim's loved one, for example.[17] Criminals will

---

[10] FTC, *Consumer Sentinel Network* (2025) (public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods).

[11] *Id.*

[12] Federal Communications Commission, *Stop Illegal Robocalls and Texts* (Feb. 27, 2026) (www.fcc.gov/sites/default/files/stop_unwanted_robocalls_and_texts.pdf); AARP, *Why You Shouldn't Answer Calls From Unknown Numbers* (July 8, 2024) (www.aarp.org/money/scams-fraud/unknown-number-do-not-answer/).

[13] Federal Communications Commission, *Stop Unwanted Robocalls and Texts* (Mar. 3, 2025) (www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts#:~:text=Don't%20answer%20calls%20from,being%20pressured%20for%20information%20immediately); AARP, *Why You Shouldn't Answer Calls From Unknown Numbers* (July 8, 2024) (www.aarp.org/money/scams-fraud/unknown-number-do-not-answer/).

[14] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[15] *Sick of Scams? Stop Answering Your Phone.*, Washington Post (June 17, 2024) (www.washingtonpost.com/technology/2024/06/17/phone-scams-dont-answer/).

[16] *Id.*

[17] Federal Trade Commission, *Scammers Use AI to Enhance Their Family Emergency Schemes* (Mar. 20, 2023) (consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes); *AI Phone Scam Mimicking Your Voice Can Now Be Used to*

often research their victims ahead of time, which they can do at scale with AI, so that their scams are highly personalized and therefore more believable.[18]

Importantly, wireless companies have taken steps to protect their customers, but they face significant challenges in defending against well-resourced, ever-evolving criminal scam operations that "continue to find new ways to reach consumers," according to the statement submitted for the JEC hearing by CTIA.[19] Companies, for example, have implemented branded calling – a paid service in which vetted companies can display their name, logo, and reason for calling on a recipient's device.[20] CTIA has called this technology "the next generation of call authentication" and claimed it was "already providing real results for millions of consumers."[21] Even some in other sectors agree that branded caller ID may be a potentially useful tool. In a joint comment submitted to the FCC in January 2026, multiple financial services industry trade associations called branded caller ID "a promising next step in the evolution of call authentication and the fight against illegal robocalls."[22]

Scam Family, Friends, Experts Warn, ABC7 (May 20, 2024) (abc7chicago.com/post/ai-phone-scam-calls-mimicking-voice-scam-family/14847406/); Federal Communications Commission, *Deep-Fake Audio and Video Links Make Robocalls and Scam Texts Harder to Spot* (June 8, 2024) (www.fcc.gov/consumers/guides/deep-fake-audio-and-video-links-make-robocalls-and-scam-texts-harder-spot); *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert).

[18] *FCC Names Its First-Ever AI Scammer in Threat Alert*, Fox News (June 5, 2024) (www.foxnews.com/tech/fcc-names-its-first-ever-ai-scammer-threat-alert); *AI Phone Scam Mimicking Your Voice Can Now Be Used to Scam Family, Friends, Experts Warn*, ABC7 (May 20, 2024) (abc7chicago.com/post/ai-phone-scam-calls-mimicking-voice-scam-family/14847406/).

[19] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[20] *Id.*; CTIA, *Branded Calling ID™ Best Practices* (Nov. 2022) (api.ctia.org/wp-content/uploads/2022/11/Branded-Calling-Best-Practices.pdf).

[21] Joint Economic Committee, Statement Submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[22] American Bankers Association et al., *Comments before the Federal Communications Commission in the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls et al.* (Jan. 5, 2026) (bpi.com/wp-content/uploads/2026/01/Joint-Trades-Urge-FCC-to-go-Further-on-Fraud-Prevention.pdf).

Still, consumer advocates, financial institutions, and other issue experts have called on telecommunications providers to take additional steps to authenticate users on their networks.[23] Hearing witness Reva Price, a Commissioner of the U.S.-China Economic and Security Review Commission and an expert on Southeast Asian scam compounds, testified during the JEC hearing that telecommunication carriers, along with social media platforms, should "implement stronger verification and detection measures."[24] Wireless providers have faced additional questions about the common industry practice of charging individual customers to access the strongest tools to protect against spam. The consumer advocacy organization PIRG, for example, has argued that "[n]o company should charge extra for essential protection services," adding, "[t]his isn't a luxury feature; it's a necessity."[25]

Our recent hearing also made clear that telecommunications companies need to take further steps to protect customers from scammers even as they serve as key partners on scams prevention for federal officials. JEC hearing witness Lois Greisman, associate director of the Division of Marketing Practices at the FTC, testified that the FTC works "very closely with the U.S. telecoms industry traceback group to identify phone scams that are coming in from abroad, hitting a gateway provider in the U.S., and to take action, whether through warning letters or law enforcement, to cut that access to the foreign networks."[26] At the same time, Richard Goldberg, associate counsel in the Fraud Section of the Department of Justice's Criminal Division, testified that telecommunications companies, along with social media and email providers, "need to continue to improve their systems to prevent victims from being reached in the first place."[27] Karen Seifert, director of the Scam Center Strike Force in the U.S. Attorney's Office for the District of Columbia, similarly argued that efforts by carriers to label suspicious phone calls are "a start, but the next step is to not even allow that phone call to come through."[28]

Expert witnesses, telecommunications providers, and other frontline industries agree that scams present an urgent and complex challenge that calls for additional action.[29] As leaders of

---

[23] *Id.*; PIRG, *Is Your Phone Company Protecting You from Scams?* (Mar. 27, 2025) (pirg.org/articles/is-your-phone-company-protecting-you-from-scams/).

[24] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[25] PIRG, *Is Your Phone Company Protecting You from Scams?* (Mar. 27, 2025) (pirg.org/articles/is-your-phone-company-protecting-you-from-scams/).

[26] Joint Economic Committee, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

[27] *Id.*

[28] *Id.*

[29] Joint Economic Committee, Testimony Submitted for the Record on Behalf of the American Bankers Association, *The Rising Global Scam Economy: Modernizing Federal*

the Joint Economic Committee, we stand ready to work together on solutions to better protect Americans from scams. To help the Committee better understand Verizon's operations and efforts to prevent scams, I seek answers to the questions below.

The following questions pertain to steps Verizon has taken to protect its customers and wireless network in the United States. Unless otherwise specified, the applicable time period is 2021 through 2025, and this request pertains to all Verizon-branded entities that provide cellular telephone service in the United States including but not limited to Cellco Partnership d/b/a Verizon Wireless. The term "communications" below refers to voice calls, including messages left on voicemail, as well as text messages, but it does not include third-party "over-the-top" messages or other messages that are received through services that Verizon does not provide directly.

1. Please describe Verizon's overall strategy for identifying and protecting its U.S. customers and network from illegal or unwanted spam and/or scam calls and texts.

    a. Please describe automated efforts and efforts which involve human review to identify illegal or unwanted spam and/or scam calls and texts, the factors Verizon uses for this identification, and the circumstances under which the company deploys these efforts.

    b. Please provide Verizon's approximate annual payroll costs, including salaries and other direct compensation to employees, consultants, independent contractors, and other workers in the U.S.
        i. What percentage of these costs are intended to protect the safety of Verizon's U.S. network and customers?
        ii. What percentage of these costs are attributable to work specifically to protect against scam communications?

    c. How much has Verizon invested per year in protecting against scam communications?

2. To the extent that Verizon attempts to identify scam attempts through calls and texts on its U.S. network:

    a. How many suspected illegal or unwanted spam and/or scam calls and texts targeting Verizon's U.S. network and customers has the company identified per year since 2021? For purposes of this question, a suspected scam call means any call that was assigned a "roboscore" or a similar metric that

---

Approaches to Protect Americans from Foreign Fraudsters, 119th Cong. (Mar. 25, 2026) (Joint Event 338091); Joint Economic Committee, Statement submitted for the Record of Sarah Leggin, CTIA Vice President, Regulatory Affairs, *The Rising Global Scam Economy: Modernizing Federal Approaches to Protect Americans from Foreign Fraudsters*, 119th Cong. (Mar. 25, 2026) (Joint Event 338091).

indicates a non-zero likelihood that the call is a scam call. The term "roboscore" has the same meaning as in Appendix A of Cellco Partnership d/b/a Verizon Wireless's Certification Pursuant to 47 C.F.R. 64.6305(d).[30]

i. What percentage of overall call and text traffic on Verizon's U.S. network per year has been suspected illegal or unwanted spam and/or scam calls and texts? Of these messages, what percentage were suspected scam activity?
ii. How much revenue has suspected illegal or unwanted spam and/or scam calls and texts on Verizon's U.S. network generated for the company per year?
iii. What percentage of suspected illegal or unwanted spam and/or scam calls and texts per year has originated from parties outside the U.S.? Please provide a geographic breakdown of this activity for each year if available.
iv. What percentage of suspected illegal or unwanted spam and/or scam calls and texts on Verizon's U.S. network has Verizon blocked?

b. Roughly how many illegal or unwanted spam and/or scam calls and texts does Verizon identify via its internal detection tools, how many are reported by customers, and how many are reported to Verizon from other sources?
i. On average, approximately how many flagged communications from users or other outside sources are reported to Verizon daily?
ii. Please describe the steps that Verizon takes once it receives reports of spam and/or scam messages from users or other outside sources, including but not limited to customers who opt to report spam on their iPhones or Android phones.
iii. Of these flagged communications, how many calls and texts has Verizon identified as being spam and/or scam activity, and how does it make that determination? Please specify if such a determination requires human review.
iv. For each communication reported to Verizon, how long on average does it take Verizon to review and make a determination that these communications are or are not spam and/or scam activity?

c. Under what circumstances does Verizon alert customers that an incoming call or text is likely an illegal or unwanted spam and/or scam communication?

3. What actions does the company take when it identifies a phone number and/or account holder on the Verizon network that is responsible for sending illegal or unwanted spam and/or scam calls and texts?

[30] Certification Pursuant to 47 C.F.R. 64.6305(d), In the Matter of Exemption from Caller ID Authentication Requirements before the Federal Communications Commission (CG Docket No. 17-97) (Feb. 26, 2026).

a. Does Verizon take steps to trace the caller/sender responsible? If so, does it work with additional parties to do so, such as the Industry Traceback Group and/or law enforcement?
    i. For Verizon customers responsible for such calls or texts, what, if any, know-your-customer information does Verizon collect that aids the company in identifying specific customers misusing its services?

b. Under what circumstances, and following what level of internal and/or external review, will Verizon suspend the account of a customer the company has determined to be responsible for sending illegal or unwanted spam and/or scam calls and texts? In your answer, please differentiate between customers who use your services for personal, household or family purposes, customers who use your services for business purposes, and reseller or wholesale customers.
    i. How many accounts has Verizon suspended per year for these reasons?
        1. How many accounts were subsequently reinstated?
        2. For accounts that were suspended and then reinstated, what is the average length of time the account was suspended?
    ii. What measures does Verizon undertake to ensure that individuals associated with these accounts and phone numbers do not attempt to create a new Verizon account or otherwise operate on the company's U.S. network?
    iii. How does Verizon implement phone number blocking? Please describe any do-not-originate and block lists that Verizon uses.

c. What efforts does Verizon undertake, if any, to determine whether accounts associated with illegal or unwanted spam and/or scam calls and texts have connections to a criminal network, a foreign government, sanctioned individuals or groups, or other individuals the U.S. has designated as threats, including Specially Designated Nationals?

d. Under what circumstances, if any, will Verizon contact law enforcement to report illegal activity on its networks, including evidence of scams?

e. Under what circumstances, if any, will Verizon report spam or illegal activity on its networks to entities that are not law enforcement, such as the FCC and CTIA's Secure Messaging Initiative?

4. Does Verizon share information with or seek information from other providers in the call path – which may include originating, terminating, gateway, and non-gateway intermediate providers, depending on the call – to help trace, track, and eliminate illegal or unwanted spam and/or scam calls and texts? Relatedly, does Verizon attempt to determine if such call providers have supported such communications, and what actions will Verizon take in response?

5. Does Verizon seek to determine if calls are made using AI-generated voices?

    a. If so, does the company alert customers when they receive a call that uses an AI-generated voice?

    b. If not, why not?

6. Verizon offers customers spam protection through its Call Filter service. The basic version of this service is available to customers for free, but the premium version requires an additional monthly fee. Regarding this service:

    a. Please describe Verizon's reasoning for charging customers for the premium version of Call Filter instead of offering comprehensive protection from illegal or unwanted spam and/or scam calls to all customers by default.

    b. What percentage of Verizon customers with eligible devices use the free version of Call Filter, the premium version of Call Filter, and no version of Call Filter at all?
        i. What spam protections, if any, does Verizon provide for customers who do not use Call Filter?

    c. Please provide the total annual gross revenue generated by customers paying for the premium Call Filter service for each year since it was first introduced.

    d. Does Call Filter come pre-loaded on eligible devices? If so, please explain. If not, why not?

    e. Does Verizon track the number of customers subscribed to the premium version of Call Filter who do not use the additional features for which they are charged?
        i. If so, does Verizon alert premium customers when they are not using the additional Call Filter features?

    f. For customers who use the free version of Call Filter, use the premium version of Call Filter, and do not use Call Filter, respectively, how many illegal or unwanted spam and/or scam texts and calls has Verizon alerted customers to each year since 2021, and how many of these texts and calls has Verizon blocked?

    g. How many customer reports of illegal or unwanted spam and/or scam calls and texts has Verizon received through Call Filter each year since it launched? How many unique phone numbers have been reported each year?

7. Is Verizon able to track how many illegal or unwanted spam and/or scam calls and texts evaded detection from its spam filters – for instance, as part of an audit of security measures? If not, why not? If so:

    a. For each year since 2021, how many unlabeled, likely illegal or unwanted spam and/or scam calls and texts reached Verizon customers who use the free version of Call Filter, use the premium version of Call Filter, and do not use Call Filter, respectively?

8. Please detail Verizon's policies and procedures with respect to customers, including businesses and charities, that send a high volume of phone calls and/or text messages. How does Verizon ensure that these customers send bulk communications only to those who have consented to receiving such messages?

9. Does Verizon limit the number of calls a wireless subscriber line can place in a single day or other interval of time?

    a. Does Verizon monitor the volume of calls placed by a wireless subscriber line as an indicator that the line is being used in a SIM farm?[31]

    b. What actions does Verizon take if it suspects a wireless subscriber line is being used in a SIM farm?

10. Please detail Verizon's policies and procedures with respect to spoofed calls, in which a caller intentionally falsifies caller ID. Specifically:

    a. What steps does Verizon take to determine the legitimacy of a spoofed call (such as a doctor's office versus a scammer)? Does Verizon specifically monitor for spoofed calls originating from abroad that present as U.S. phone numbers? If not, why not? If so, what is Verizon's success rate for identifying such calls, and what action does the company take when it detects these calls?

    b. Does Verizon specifically monitor for spoofed caller IDs that misrepresent callers as an existing entity, such as a bank or federal agency? If not, why not? If so, what action does it take when it detects these calls?

---

[31] According to PBS, "SIM farms are hardware devices that can hold numerous SIM cards from different mobile operators. These devices then exploit voice over internet protocol (VoIP) technology to send and receive bulk messages or calls. While initially developed for legitimate purposes, such as low cost international calling, the technology has become a cornerstone of organized fraud targeting mass audiences — phishing texts and scam calls." *How 'SIM Farms' Like the One Found Near the UN Could Collapse Telecom Networks,* PBS (Sept. 23, 2025) (www.pbs.org/newshour/nation/how-sim-farms-like-the-one-found-near-the-un-could-collapse-telecom-networks).

11. Verizon acknowledges that "most messages sent via email-to-text are from spammers."[32] What steps, if any, does Verizon take to identify and prevent the misuse of the email-to-text feature, which allows users to send text messages via an email?

    a. Does Verizon enable email-to-text capabilities by default for customers using eligible devices?
        i. If so, what percentage of customers, on average, opt out of using email-to-text?
        ii. If not, what percentage of customers, on average, opt in to using the email-to-text feature?

12. In 2025, Verizon announced it was launching Branded Calling ID™ on its network.[33]

    a. What company/companies does Verizon contract with to deliver branded calls?

    b. How does Verizon, or any company it contracts with to deliver branded calls, vet companies seeking to send branded calls on its network?

    c. If Verizon has reason to believe that a branded call on its network is illegitimate, what steps does it take?

    d. How much does Verizon charge businesses to place branded and un-branded calls, respectively, on Verizon's network?

Please provide your responses as soon as possible but in no event later than June 11, 2026. If you have any questions related to this request, please contact [redacted]

[32] Verizon, *Manage Email-To-Text Opt-In and Opt-Out* (www.verizon.com/about/account-security/email-to-text-faqs) (accessed Feb. 2, 2026).

[33] CTIA, *New Consumer Tool, Branded Calling ID™ to Launch on Verizon's Network* (Sept. 15, 2025) (www.prnewswire.com/news-releases/new-consumer-tool-branded-calling-id-to-launch-on-verizons-network-302556438.html).

Sincerely,

David Schweikert
Chairman

Margaret Wood Hassan
Ranking Member

cc: Eric Schmitt
Vice Chairman, Joint Economic Committee