



# SCAM ROBOCALLS:

TELECOM PROVIDERS PROFIT



June 2022

## ABOUT THE NATIONAL CONSUMER LAW CENTER

Since 1969, the nonprofit National Consumer Law Center® (NCLC®) has used its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people in the United States. NCLC's expertise includes policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services; and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, and federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness.

**NCLC.ORG**

## ABOUT THE ELECTRONIC PRIVACY INFORMATION CENTER

Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., focused on emerging privacy and technology issues. Since 1994, EPIC has worked at the intersection of policy, advocacy, and litigation. EPIC litigates cases on emerging privacy issues, provides expert advice to policymakers, lawmakers, courts and litigators, and facilitates dialogue between advocates, experts, and decisionmakers. EPIC has worked for strong consumer protections against unwanted and illegal calls through numerous amicus briefs, public comments, and attorney trainings.

**EPIC.ORG**

© Copyright 2022, National Consumer Law Center, Inc. and Electronic Privacy Information Center. All rights reserved.

## ABOUT THE AUTHORS

**Margot Saunders** is currently Senior Counsel to the National Consumer Law Center (NCLC) after serving as managing attorney of NCLC's Washington, D.C. office from 1991 to 2005. Margot has testified before Congress more than two dozen times regarding a wide range of consumer law issues, including predatory mortgage lending, high cost small loans, payments law, electronic commerce, protecting benefits in bank accounts, privacy issues, and for the past several years--robocalls. She was the lead advocate on the passage of the Home Ownership and Equity Protection Act, the development of the Treasury Rule protecting exempt benefits, and many other initiatives. Margot has served as an expert witness in over 50 consumer credit cases in more than 20 states, providing opinions on predatory lending, electronic benefits, servicing, and credit math issues in individual and class cases. She is a co-author of NCLC's [Consumer Banking and Payments Law](#), many articles, and a contributor to numerous other manuals. Prior to joining NCLC, she was the consumer law specialist for North Carolina Legal Services. In 1991, Margot was the second recipient of the Vern Countryman Award. She is a graduate of Brandeis University and the University of North Carolina School of Law.

**Chris Frascella** is a Law Fellow in Telephone Subscriber Privacy at the Electronic Privacy Information Center (EPIC), where his work focuses primarily on robocalls and data brokers. Chris has contributed to multiple amicus briefs explaining the technology and policy underlying the Telephone Consumer Protection Act (TCPA), and has submitted comments to state and federal agencies on topics including robocalls, SIM swapping, prison phone surveillance, fraudulent emergency data access requests, broadband privacy, and app-based payment platforms. As a law student, his internship experiences included the Federal Trade Commission's Bureau of Consumer Protection, the Office of Consumer Protection within the DC Office of the Attorney General, the Bureau of Internet and Technology (BIT) within the NY Attorney General's Office, the Administrative Conference of the United States (ACUS), and the Office of Privacy and Civil Liberties within the U.S. DOJ. Prior to law school, Chris worked for nearly a decade in digital marketing for software startups. He is a graduate of the George Washington University Law School, American University, and Fordham University.

## ACKNOWLEDGEMENTS

The authors would like to thank NCLC Deputy Director Carolyn Carter and EPIC Senior Counsel Megan Iorio for their invaluable analysis, advice, and reviews; Maggie Westberg, NCLC's Research Assistant for compiling the information in Appendix 2, Alinnah Qiao, Executive Assistant at EPIC for proofreading assistance with Appendix 2, and Emily Caplan for essential citation checks and corrections. The authors would also like to extend their special thanks for the creativity and expertise shared by David Frankel, CEO of ZipDX, and Ted Hobson, an attorney with the Consumer Assistance Program in the Vermont Attorney General's Office (whose contributions were his own personal opinions and are not necessarily shared by the Vermont Attorney General). Additionally, we very much appreciate the illustrative data provided by Mike Rudolph, CTO of YouMail. We appreciate the indispensable assistance of NCLC's communications and operations team, Michelle Bates Deakin, Stephen Rouzer, and Moussou N'Diaye, and we'd like to thank Julie Gallagher for layout and design assistance. The views expressed in this report are solely those of NCLC and EPIC and the authors.

# SCAM ROBOCALLS:

## TELECOM PROVIDERS PROFIT

### TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY</b>	3
<i>What needs to be done to stop the fraudulent calls.</i>	5
<b>I. AMERICANS ARE LOSING BILLIONS OF DOLLARS EVERY YEAR FROM SCAM ROBOCALLS.</b>	6
A. <i>There are billions of scam robocalls every year.</i>	6
B. <i>Scam robocalls cost American subscribers almost \$30 billion in 2021.</i>	8
<b>II. SCAM TEXTS ARE INCREASING.</b>	10
<b>III. HOW DID THE U.S. TELEPHONE SYSTEM BECOME SUCH A MESS?</b>	11
A. <i>Providers' choices determine whether scam calls reach subscribers.</i>	11
B. <i>U.S. providers are complicit in routing illegal robocalls originating in the U.S. and abroad.</i>	12
C. <i>Tracebacks reconstruct the call path of illegal robocalls.</i>	14
D. <i>Providers are aware of their role in delivering illegal calls.</i>	16
E. <i>Providers have a system to filter out some spam texts, but it is insufficient.</i>	18
<b>IV. THE U.S. GOVERNMENT HAS NOT BEEN ABLE TO STOP THE SCAM CALLS.</b>	19
A. <i>The Federal Communications Commission's (FCC's) approach to regulating robocalls has not solved the problem.</i>	19
B. <i>The Federal Trade Commission's (FTC's) enforcement of the Telemarketing Sales Rule (TSR) is unlikely to stop the illegal calls.</i>	25
<b>V. THE FCC CAN STOP MOST SCAM ROBOCALLS AND ILLEGAL TEXTS—HERE IS HOW.</b>	26
<b>ENDNOTES</b>	31

## APPENDICES

<b>APPENDIX 1</b>	<b>Other Invasive Robocalls</b>	46
<b>APPENDIX 2</b>	<b>Scam Robocalls in the States</b>	50

## TABLES

<b>TABLE 1</b>	<b>Total Annual Scam Robocalls 2018 Through 2021</b>	6
<b>TABLE 2</b>	<b>Rate of Complaints to FTC About Scam Calls and Scam Texts from 2017 to 2021</b>	8
<b>TABLE 3</b>	<b>Number of Americans that Lost Money to Scam Calls</b>	9
<b>TABLE 4</b>	<b>Total Losses from Scam Calls</b>	9
<b>TABLE 5</b>	<b>Call Path from Foreign Originating Provider to Terminating Provider</b>	12
<b>TABLE 6</b>	<b>Comparing Legal Robocalls to <i>Illegal</i> Robocalls</b>	17









## EXECUTIVE SUMMARY

*Every month, more than one billion scam robocalls designed to steal money from unsuspecting telephone subscribers are made possible because providers—typically small, pop-up VoIP telephone providers—transmit these calls through to our telephones. Every answered scam robocall pays money to those providers, as well as to every telephone service provider in the call path.*

*Even when these providers are told—sometimes repeatedly—that they are transmitting fraudulent calls, they keep doing it, because they are making money from these calls. And even when they are caught and told to stop, they are not criminally prosecuted, and the fines that are levied are rarely collected. FCC Commissioner Geoffrey Starks has noted this counterproductive dynamic regarding robocalls: “[I]llegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it.”*

*This report explains the depth of the problem, the reasons for the problem, and how the Federal Communications Commission has responded. We recommend several simple strategies that would stop most, if not all, of these fraudulent robocalls.*

**Problem:** Every month well over one billion scam robocalls—calls to defraud telephone subscribers—are made to American telephones. This is more than 33 million scam robocalls every day. Criminals make these calls to scare or trick Americans into turning over hundreds or even thousands of dollars.

Typical frauds include calls scaring seniors into believing that unless they turn over thousands of dollars they will lose access to their [Social Security](#)  or [Medicare benefits](#) ; threats to immigrants that if they don't pay the caller they will be deported; and calls in which the recipient is tricked into believing they have been refunded too much money by [Amazon](#)  or [Apple](#) , requesting that the excess be returned. Other typical scams include selling phony [health insurance](#) , calls purporting to be from the [IRS](#) , [student loan scams](#) , threats of arrest, debt reduction scams, and scam telemarketing calls (such as the ubiquitous [auto warranty call](#) ). These scam robocalls are in addition to the annoying, but not necessarily illegal, calls from debt collectors, people taking surveys, and charities summarized in Appendix 1. Scam texts are also increasing, and are similarly effective in stealing money from consumers.

Look for the  to listen to recordings of real robocalls attempting to scam consumers.

Last year almost **60 million Americans** lost over **\$29 billion** to these scam callers. More than one million complaints were made to the FTC about scams from calls and texts.



Illegal calls impair the value and efficiency of the U.S. telephone system. The problem has become so pervasive that 70% of Americans do not answer calls from numbers they do not recognize. This increases costs for health care providers, small and large businesses, and their call recipients, who miss or incur delays in receiving time-critical communications for fear of answering a robocaller. These unwanted calls are also a prime reason that many landline subscribers are dropping their landline subscriptions.

**Causes.** One cause of this current mess is the deregulation of the American telephone system, which has deregulated the call path for long distance calls. Rather than a single telephone company transferring the calls directly from the caller to the called party, multiple providers transmit calls from the caller to the called party. Each transfer of the calls from one provider to the next involves a separate agreement between the providers, which determines the price the upstream provider will pay the next downstream provider to transfer the calls. This process also allows downstream providers to refuse to take calls from upstream providers if they do not like the price offered for the transmittal, or if they deem the calls potentially illegal—and thus too costly.

Another cause is the development of VoIP (a technology that accesses the telephone network through the internet), which allows callers to reach U.S. telephone subscribers with minimal expense. Many small VoIP providers are honest businesses, but a few are complicit in facilitating the fraudulent calls. Unlike large, facilities-based telephone providers, small VoIP providers often set up service in temporary quarters or their home and offer their services through online advertisements. Once caught facilitating scam calls, they need only change their name to pop up under a different business identity and continue operations.

The telecom industry continues to transmit tens of billions of illegal calls each year because every answered call provides revenue for the transmitting voice service providers. Each provider in the call path makes a fraction of a cent for every answered call that it transmits. While the terminating providers strive to block illegal calls, the complicit originating provider and some intermediate providers find it profitable to continue processing these calls. Providers can choose not to accept fraudulent robocalls from upstream providers, but they need to be incentivized to reject these calls.

**Government Response.** Congress passed the Telephone Consumer Protection Act (TCPA) in 1991 to limit unwanted calls by requiring that callers have prior express consent for autodialed calls to cell phones and prerecorded calls to cell phones and residential lines. In 2019, Congress passed the TRACED Act, requiring—among other things—that the FCC issue regulations to authenticate the caller IDs shown on telephone calls (known in the industry as STIR/SHAKEN), establish a method to trace the sources of illegal calls by naming

an “Industry Traceback Group” (ITG), and require providers to respond to ITG requests for information about illegal calls.

The FCC has initiated regulatory efforts and enforcement actions aimed at controlling these illegal calls. Yet, every month, well over a billion scam robocalls continue to ring on the telephones of U.S. subscribers.

The problem is that applying the STIR/SHAKEN methodology requires only that originating providers apply a certification indicating how confident they are that the caller ID displayed in the calls is correct. It does not cause the scam calls to stop. And the FCC’s pending regulatory efforts would continue to require only that providers have procedures in place to mitigate illegal robocalls, with no meaningful and enforceable requirement that these procedures actually be effective.

### *What Needs to Be Done to Stop the Fraudulent Calls.*

Providers choose whether to accept calls from upstream providers. These decisions are now generally based only on the prices upstream providers pay for processing their calls down the call path toward the recipient. This dynamic is key: the rules governing the process used by providers must provide strong incentives for all providers in the call path (from caller to called party) to *refuse to transmit calls likely to be illegal*.

There are multiple tools available to providers that inform them about the potential illegality of the calls coming their way. These include information from tracebacks done by the Industry Traceback Group about which providers have transmitted illegal calls, examination of the provider’s call detail records, and analysis of the content of the calls (available through various industry service providers).

If these crimes were occurring in the physical world, rather than over the telephone and internet, law enforcement would not hesitate to arrest the thieves and their helpers to stop them from stealing. The FCC should provide the same level of protection to American telephone subscribers.

We propose three principles to stop the criminal robocalls:

1. All providers in the call path should have an affirmative obligation to engage in effective mitigation against illegal robocalls.
2. Providers who knew or should have known that they were transmitting illegal robocalls should face clear financial consequences.
3. Law enforcement, telephone service providers, victims of scam calls, legal robocallers, and the general public should have access to all available information about the sources of the illegal robocalls and their complicit providers.

Our five specific proposals to accomplish these principles are included on [page 26](#).

## I. AMERICANS ARE LOSING *BILLIONS* OF DOLLARS EVERY YEAR FROM SCAM ROBOCALLS.

Every call we receive that uses a prerecorded or artificial voice is a “robocall.”<sup>1</sup> Not every robocall is annoying—we appreciate the reminders from our doctor’s office or the warning from the airline that our flight is late. But unwanted robocalls are invasive and aggravating. And some are outright attempts to defraud us.

Robocalls, whether made to cell phones or to landlines, are governed by the Telephone Consumer Protection Act (TCPA) passed by Congress in 1991.<sup>2</sup> Most are legal only if the recipient has provided *prior express consent* for the call or if the Federal Communications Commission (FCC) has exempted the particular type of call from this requirement.<sup>3</sup>

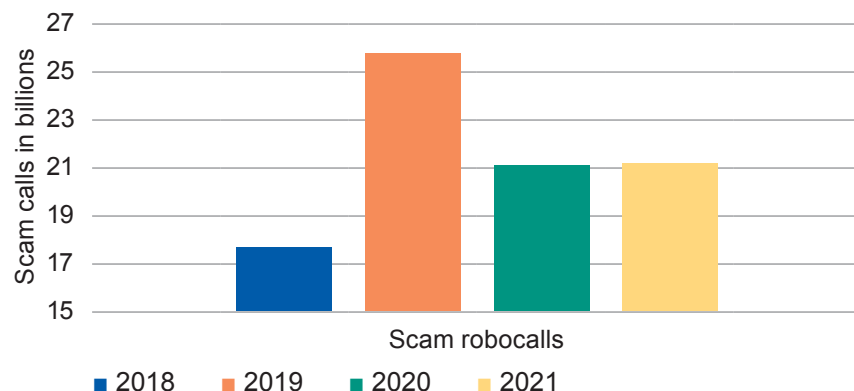
This report is about robocalls that perpetrate frauds against telephone subscribers—scam robocalls. The number of these scam robocalls continues to escalate, and Americans are losing an increasing amount of money to scam robocalls.<sup>4</sup>

### A. *There are billions of scam robocalls every year.*

*More than **one billion scam robocalls**<sup>5</sup> are made to American telephones every month, all seeking to defraud American telephone subscribers. This is over 33 million scam robocalls every single day. (See Appendix 2 for illustrations of scam robocalls in each state.)*


TABLE 1

#### Total Annual Scam Robocalls 2018 Through 2021<sup>6</sup>




Scam robocalls assault seniors, immigrants, people with disabilities, student loan borrowers, and any recipient of the call. The top 1,000 scam robocall campaigns are responsible for a large percentage of scam robocalls.<sup>7</sup> Examples of typical robocall scams include:








**Scams against seniors.** In a standard senior scam scenario, a **prerecorded call**  from someone claiming to be from the Social Security Administration is answered by a senior citizen. This happened recently to a retired Virginia woman in her 60s caring for her disabled son; she received a robocall purportedly from the Social Security Administration with a message that federal drug agents had found her information connected to a car transporting cocaine. Alarmed, she responded, and then fell victim to the scammer, who swindled her out of most of her nearly \$445,000 in savings. She now lives on her son's disability payments and her Social Security.<sup>8</sup>


This type of scam is all too frequent. Hundreds of thousands of calls are made every month to seniors threatening arrest or suspension of benefits for a fictitious problem with Social Security benefits.<sup>9</sup> Complaints made by seniors to the FTC about scams in general are increasing. Seniors reported over \$1 billion in fraud losses in 2021.<sup>10</sup>



**Scams against immigrants.** One horrific scam against immigrants starts with robocalls in Mandarin to Chinese immigrants. The message purports to be from the Chinese Consulate, and the victims are told, "There is an important document that needs to be picked up; it may affect your status in the U.S.; press a button to speak with a specialist." When the immigrant presses the button, the connection is made to a live scammer. In one example of this scam, a 65-year-old Chinese immigrant in New York was scammed out of \$1.3 million after receiving Chinese-language robocalls claiming that she was being investigated for financial crimes in China.<sup>11</sup>

**Scams against people with disabilities.** Every month, there are millions of **scam calls**  offering fake assistance applying for Social Security disability benefits where the true goal of these calls is to gain the recipient's personal information to steal their identity.<sup>12</sup>

**Scams against student loan borrowers.** Typically, these **scam calls**  attempt to scare the recipient into answering the call with the threat of a collection action or termination of a payment suspension. The goal is to solicit personal information to facilitate identity theft.<sup>13</sup>

**Scams against anyone who answers the telephone.** Leading scam robocalls that are not specifically targeted include **vehicle warranty** ,<sup>14</sup> **Medicare** ,<sup>15</sup> **health insurance** ,<sup>16</sup> and **bill reduction**  scams.<sup>17</sup> Other common types of scam robocalls are government imposter scams

Look for the  to listen to recordings of real robocalls attempting to scam consumers.

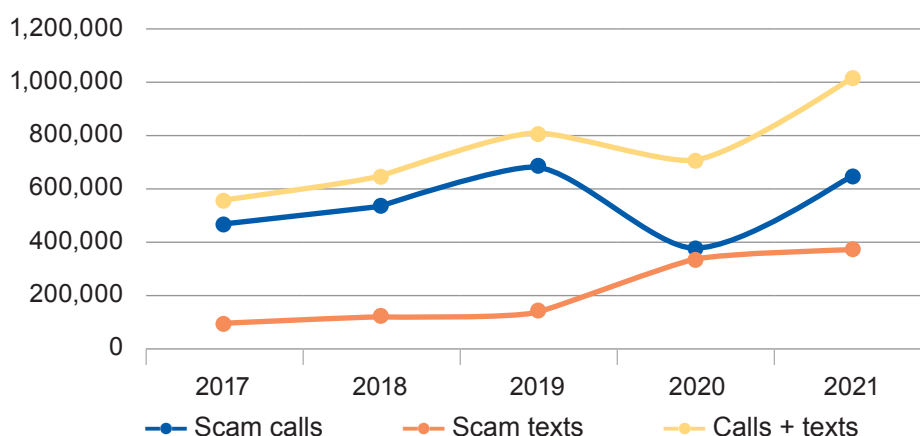
(e.g., calls purporting to be from the [IRS](#) <sup>18</sup>) and calls impersonating a business such as [Amazon](#) <sup>19</sup>. For *each* of these types of scam robocalls, tens of thousands (sometimes hundreds of thousands) of calls are made to American telephone subscribers *every month*.<sup>20</sup> More stories about these scam calls are included in the state pages in Appendix 2.

Scam callers typically use disguised caller IDs to hide the real number used to make the call and their identity.<sup>21</sup> Often the caller spoofs the telephone number of a trusted source, such as the Social Security Administration, the IRS, or a local hospital, or uses a number that makes it appear that the caller is someone in the called party's neighborhood.<sup>22</sup> Scam callers increasingly “rent” a large block of telephone numbers, sometimes changing to a different number for each call, in order to make it harder to identify the calls as scam calls or block them.<sup>23</sup>

The Federal Trade Commission (FTC) reported 644,048 complaints of fraud attempted through a phone call and another 377,840 about texts to cell phones, totaling over 1 million. This was an increase of 37% from the previous year.<sup>24</sup> While not all of the complaints were about scam robocalls (some may have been about live calls), applying Truecaller's estimate that 60% of scam calls are robocalls,<sup>25</sup> that means that in 2021 there were more than 386,500 complaints about scam robocalls.<sup>26</sup>

TABLE 2

### Rate of Complaints to FTC About Scam Calls and Scam Texts from 2017 to 2021<sup>27</sup>

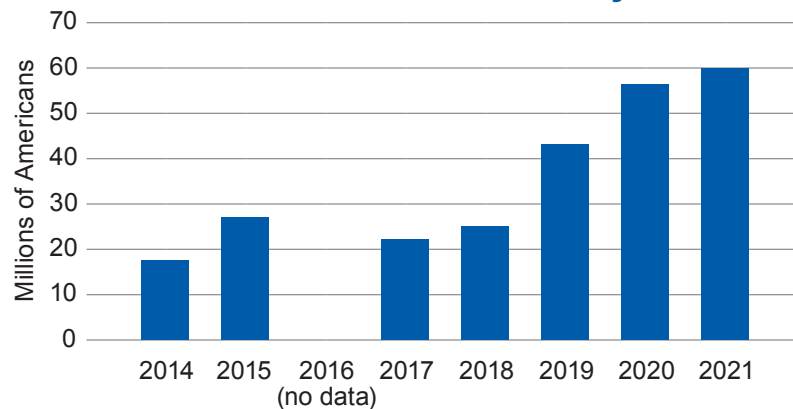


### ***B. Scam robocalls cost American subscribers almost \$30 billion in 2021.***

Harris Poll surveys show that **59.4 million Americans were victims of fraud through calls or texts in the 12-month period ending in June 2021.**<sup>28</sup>

TABLE 3

### Number of Americans that Lost Money to Scam Calls<sup>29</sup>



This data shows that U.S. telephone subscribers had an estimated **\$29.8 billion stolen through scam calls in the 12 months before June 2021**, an increase of over 50% in just one year.<sup>30</sup> Even the FTC's data, based just on losses affirmatively reported by consumers, documents that \$692 million was stolen in 2021 through **scam calls**.<sup>31</sup> The FTC reports the median amount lost by each victim to scam calls was \$1,200 in 2021.<sup>32</sup> And, the FTC found that those over 80 years of age lost an average of \$1,500 to scams in 2021.<sup>33</sup> In a special report on scams against seniors completed in 2021, the FTC found that for consumers over age 60, the median loss from scam calls was \$1,800, and for consumers over age 80, the median loss from scam calls was nearly twice as high at \$3,000.<sup>34</sup>

TABLE 4

### Total Losses from Scam Calls<sup>35</sup>

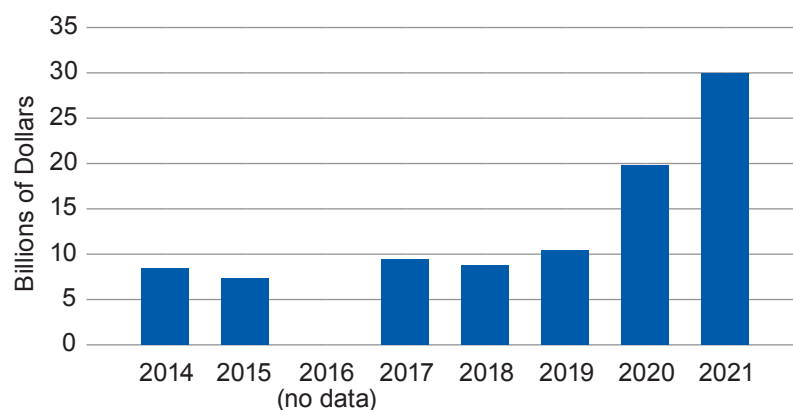


Table 4 illustrates the dramatic growth in losses suffered by the *direct victims* of fraudulent calls. However, defrauded American telephone subscribers are not the only losers from illegal calls. Even consumers who are not duped by these calls

suffer costs in the form of wasted time and nuisance—that the FCC estimates amount to at least \$3 billion annually.<sup>36</sup>

Robocalls are a major cause of the degradation of the U.S. telephone network. The problem has become so pervasive that 70% of Americans do not answer calls from numbers they do not recognize.<sup>37</sup> One hospital reported persistent inability to reach patients due to call screening.<sup>38</sup> Contact tracing efforts during the first months of the COVID-19 pandemic were also severely impacted by phone subscribers refusing to pick up because they expected a call from an unknown number to be a waste of their time.<sup>39</sup> Unwanted calls are also a prime reason why many landline subscribers are dropping their landline subscriptions.<sup>40</sup>

## II. SCAM TEXTS ARE INCREASING.

Scammers are increasingly moving towards texts as a way to avoid the protections erected against illegal robocalls.<sup>41</sup> To avoid detection, text scammers are using the same methods callers use to spoof telephone numbers.<sup>42</sup>

In a typical text scam, a scammer sends an alluring text message inviting the recipient to click on a link, which initiates a fraudulent transaction with the scammer.<sup>43</sup> Fraudulent texts take many forms, including messages impersonating package delivery companies or appearing to advertise real items for sale.<sup>44</sup>

The number of complaints to the FTC about scam texts rose to 377,840 in 2021, up by over 12% in one year, and by a whopping 315% since 2017.<sup>45</sup> (This is illustrated in Table 2, *supra*.) Similarly, complaints made in 2021 to the FCC about unwanted texts (many of which are likely to have been scams) rose by over 143% between 2017 and 2021.<sup>46</sup>

**The most unfortunate consequence of the rise in spam texts is the dramatic increase in *direct consumer losses from scams and frauds perpetrated by those texts*. In 2021, victims reported losses of \$131 million, a 254% increase from 2017.**<sup>47</sup> The actual losses to American consumers are likely even greater than this figure, as only a small percentage of fraud is reported.

Texts are treated as “calls” under the Telephone Consumer Protection Act (TCPA).<sup>48</sup> As a result, a text can be sent to a cell phone using an “automated telephone dialing system” (ATDS) only with the recipient’s prior express consent.<sup>49</sup> In addition, whether or not it is autodialed, a text that includes a telemarketing message cannot legally be sent to a cell phone that is considered a residential line and is registered on the National Do Not Call Registry.<sup>50</sup> But some courts interpret the U.S. Supreme Court’s 2021 decision in *Facebook, Inc.*

*v. Duguid*<sup>51</sup> in such a narrow way that the ATDS definition does not apply to the autodialers used today to send mass texts.<sup>52</sup> And the Do Not Call registry applies only to residential lines, and only to messages “for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services. . . .”<sup>53</sup> Moreover, the entities sending scam texts are typically located overseas, are adept at evading identification, and generally ignore all aspects of the FCC’s rules. As a result, the TCPA’s restrictions provide little effective protection from scam texts for American consumers.

### III. HOW DID THE U.S. TELEPHONE SYSTEM BECOME SUCH A MESS?

Voice service providers determine whether scam calls reach consumers’ phones. Call traffic of any kind (legal or illegal) translates into profit for smaller providers. Even when scam calls are traced back through their networks, or when they are notified of illegal call traffic by other means (such as their own analytics tools or other protocols they certify are part of their robocall mitigation program), these providers continue to let these calls through, prioritizing their own revenue because their stake in the harm to consumers is negligible.

#### *A. Providers’ choices determine whether scam calls reach subscribers.*

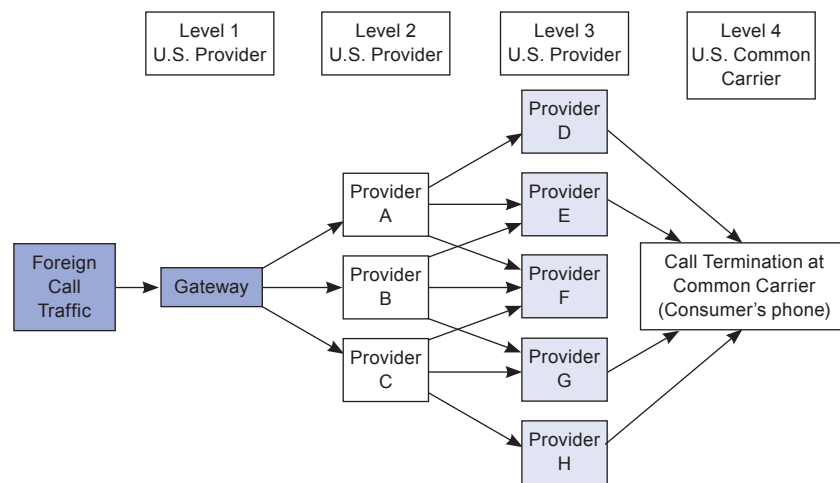
Decades ago, consumers paid as much as \$0.25 per minute for local calls,<sup>54</sup> with increased rates for long distance calls.<sup>55</sup> Today, because “wholesale rates to U.S. mobile phones are less than a penny per minute and accessible virtually worldwide,”<sup>56</sup> consumers pay much lower telephone costs for local and long distance calling.

The reduction in the cost of long distance calling is a function of changes in how long distance calls are routed from the caller to the called party. Rather than a single telephone company transferring the calls directly from the caller to the called party, calls now pass through multiple providers. Calls enter the U.S. telecommunications network through an “originating provider,” which provides service directly to callers,<sup>57</sup> or through a “gateway provider,” a U.S. telecommunications company that receives a call that originates overseas.<sup>58</sup> This provider passes the call downstream to an “intermediate” provider,<sup>59</sup> which then chooses, in turn, the next intermediate provider that will transmit the call down the call path toward the recipient. At the end of the call path, often after many hops from one intermediate provider to another, the call reaches the “terminating provider,” which routes the call to the called party.



All of these transfers are made pursuant to agreements between the providers, setting forth the price the upstream provider will pay the next downstream provider for accepting and transmitting the calls. Each carrier in the call path generally seeks “least cost routing,”<sup>60</sup> thus spurring competition to offer lower rates per call. This process also allows downstream providers to refuse to take calls from upstream providers if they do not like the price offered for the transmittal, or if they deem the calls potentially illegal—and thus too costly.

TABLE 5  
**Call Path from Foreign Originating Provider  
to Terminating Provider<sup>61</sup>**



This process allows telephone users to receive the benefits of the increased competition among the providers. But letting market dynamics determine a call's path also creates new ways for bad actors to process scam calls to victims. A single successful fraud resulting from one call out of half a million robocalls more than covers the slight expense of the entire high-volume scam robocall campaign.<sup>62</sup>

***B. U.S. providers are complicit in routing illegal robocalls originating in the U.S. and abroad.***

Approximately half of the callers making government and business imposter calls are located overseas. To reach American telephones, the calls must be transmitted through a gateway provider based in the U.S.<sup>63</sup> Typically, these providers, the originating providers that service fraudulent robocallers, and the first few intermediate providers for these calls, are small companies using VoIP (Voice over Internet Protocol) services.<sup>64</sup>

*“In the course of this investigation, I learned that with little more than off-the-shelf VoIP technology, an autodialer, and a business relationship with a gateway carrier, any individual or entity with a broadband internet connection can introduce unlimited numbers of robocalls into the U.S. telephone system from any location in the world.”—Marcy Ralston, Special Agent, Social Security Administration, Office of the Inspector General*<sup>65</sup>

VoIP is a technology that accesses the telephone network through the internet, and is commonly used by many large telecommunications providers in place of traditional landlines to provide service to residential and business customers. Often, the telephone service is paired with internet access and cable television service.

The VoIP providers that process the illegal robocalls are generally small, often simply one or two individuals with minimal investment or technical expertise who have set up a service in their home or other temporary quarters and offer services through online advertisements.<sup>66</sup> These small VoIP providers are often called “nomadic” VoIP services<sup>67</sup> to distinguish them from the much larger “fixed interconnected VoIP service” providers that tend to be fairly large companies such as AT&T<sup>68</sup> or Xfinity,<sup>69</sup> which own their own equipment and provide fixed telephone numbers with service to landline telephone customers.<sup>70</sup>

While some small VoIP providers strive to allow only law-abiding callers into the network, some of them deliberately turn a blind eye to patently illegal traffic.<sup>71</sup> These complicit VoIP providers send their calls to larger voice service providers (VSPs), who in turn transmit the calls to the terminating providers.

As explained by the Vermont Attorney General in a recently filed complaint against a small VoIP provider, a “fraudulent robocall now most frequently ‘hops’ from a foreign entity to a domestic voice service provider (as the U.S. point of entry), then on through multiple domestic intermediary domestic providers to a large domestic carrier—such as Verizon Wireless or AT&T—that ultimately terminates the call with connection to an actual phone.”<sup>72</sup>

The transmission of illegal, fraudulent robocalls typically works like this:

- First, a foreign originating provider transmits an illegal robocall campaign and sends it over the internet to a U.S. based VoIP service—the gateway provider.<sup>73</sup>
- Alternatively, a U.S. originating provider originates the call and sends it to a different U.S. based provider. Sometimes, however, calls may flow from the U.S. to foreign providers and then back into the U.S. in an attempt to hide the identity of the real originating provider.<sup>74</sup>
- Typically, robocalls travel from smaller U.S. providers to larger U.S. providers, and then on to the terminating provider that delivers the call to the subscriber.<sup>75</sup>

- In each transition from one provider to the next, the sending provider is charged something for each call by the receiving provider.<sup>76</sup>

As the calls move from originating or gateway provider to the first intermediate provider, and then on down the line to subsequent intermediate providers, they are mixed with calls from other providers. Because some intermediate providers accept both illegal traffic and legal calls (both automated and conversational traffic), calls from different sources get blended together as traffic passes from provider to provider, making identification of fraudulent calls most difficult for terminating *providers furthest removed from the source of the scam calls*.

Fraudulent callers also spoof caller IDs to make detection more difficult.

A cottage industry has developed for VoIP providers who offer “dialer traffic” to facilitate both legal automated calls as well as the fraudulent calls plaguing American telephones.<sup>77</sup> The legal calls provide cover for the illegal calls. Some of the VoIP providers involved in these calls explicitly present their services as especially valuable for callers making illegal calls who are seeking to avoid the efforts of the downstream providers who try to protect their subscribers from mass scam robocall campaigns.<sup>78</sup> For example, some advertise and provide a service that allows their robocalling customers to use a different caller ID for each robocall,<sup>79</sup> as a way to avoid the blocking and labeling efforts used by the downstream service providers striving to protect their customers from these scam calls.<sup>80</sup> By contrast, legitimate telemarketing robocallers tend to rely on consistent use of a relatively small set of caller IDs for outbound call campaigns to track the effectiveness of their efforts.<sup>81</sup>

Originating providers, gateway providers, and at least the first intermediate provider that receives the calls from the originating or gateway providers should be fully aware of the nature of the fraudulent calls being transmitted, if they paid any attention. As explained in the next two subsections, multiple tools are already available to providers that try to avoid transmitting fraudulent robocalls. Without the complicit gateway and intermediate voice service providers based in the U.S., few foreign fraudulent robocalls would ever reach American telephones.<sup>82</sup>

### **C. Tracebacks reconstruct the call path of illegal robocalls.**

To find the criminal callers and their complicit providers, the TRACED Act required the FCC to select a group to conduct tracebacks of suspected unlawful robocalls.<sup>83</sup> The FCC selected USTelecom,<sup>84</sup> a trade association for telephone companies and providers of broadband services, to be the Industry Traceback Group (ITG).<sup>85</sup>

Tracebacks work like this:

- Using a secure portal, the ITG contacts the terminating provider that delivered the unlawful call to the consumer and gives that provider (1) the time and date of the call, (2) the calling number, (3) the called number, (4) the specific nature and content of the illegal robocall in question, and (5) the likely laws violated by the call.<sup>86</sup>
- ITG then asks that terminating provider to identify the upstream voice service provider that transmitted the call to it. Once the carrier identifies which upstream provider routed the call to it, ITG contacts *that* upstream provider using a database tool. As it did with the previous carrier, ITG provides notice of the nature and content of the illegal robocall, including a link to a recording of the call, and asks the upstream provider to identify which further upstream provider routed the call to it.<sup>87</sup>
- In turn, each voice service provider in the call path provides the ITG with the identity of the upstream voice service provider from whom it received the suspicious traffic and enters the information into the portal.<sup>88</sup> The process continues until the originating voice service provider is identified or a dead end is reached.<sup>89</sup>

As the Vermont Attorney General explained in a recent complaint filed against a complicit gateway provider:

*By this method, ITG “asks” its way up the call-path, identifying each of the domestic . . . [voice service providers] involved in facilitating the illegal robocall in question, and [putting] each on notice of the nature and content of that call. At some point in most tracebacks of government or business imposter fraud, a domestic [voice service provider] reports to ITG that it received the call from a foreign customer. Thus, ITG—under FCC authority—identifies the . . . [voice service provider] that served as the U.S. point of entry to the illegal robocall.*<sup>90</sup>

Each traceback is of a single telephone call. But robocalls, by their very nature, are never made by themselves. Each robocall is indicative of thousands of similar—usually identical—calls, with the only difference being the recipient of each call. As a result, when the ITG identifies which U.S. voice service provider routed a single illegal robocall into the U.S. from abroad, the ITG has identified the provider that delivered a torrent of illegal calls to American telephones.

The ITG traced 2,500 calls determined to be illegal in 2020<sup>91</sup> and 2,900 calls in 2021.<sup>92</sup> The ITG traceback process informs the ITG and the FCC of the service providers that are the sources of these illegal calls: either the U.S. based originating providers or the gateway providers.

The traceback process also informs each of the voice service providers in the call path, including all the intermediary providers, that a traceback through that provider's system is being conducted, and that the traceback relates to an illegal robocall. As explained in the complaints filed by both the North Carolina and Vermont Attorneys General, the ITG provides a notice to each provider in the call path explaining that they have transmitted "suspected and known fraudulent and/or illegal robocalls."<sup>93</sup> The ITG usually sends to each provider a link to an audio recording of the illegal robocall.<sup>94</sup>

#### *D. Providers are aware of their role in delivering illegal calls.*

**Tracebacks.** The providers that are complicit in transmitting illegal calls are well aware of what they are doing. They know that the calls are illegal because they have received multiple traceback requests. With each traceback request,<sup>95</sup> they are given a notice from the ITG that they are transmitting suspicious calls.<sup>96</sup> **So, even if the providers did not know before they received the traceback request from the ITG that the calls transmitted over their networks were illegal, the providers are fully aware once the traceback requests start arriving.**

Intermediate providers are also complicit if they continue transmitting calls from gateway or originating providers after receiving notices that calls they received from those providers were the subject of multiple traceback requests. For example:

- In a case against gateway provider Startel brought by the Indiana Attorney General, a defendant downstream intermediate provider, Piratel, received four traceback requests in three weeks about calls it accepted from Startel.<sup>97</sup>
- In a case brought against Articul8, another intermediate provider, by the North Carolina Attorney General, the defendant had received 49 traceback requests.<sup>98</sup>

**Behavioral Analytics.** Providers need not wait to receive a traceback request from the ITG to know that the calls they are transmitting are illegal. The providers have specific tools to evaluate on a granular level which robocalls are illegal. Every provider maintains Call Detail Records (CDRs) for each and every call. (It is through the CDRs that the providers are paid for their calls and the traceback process is conducted.) The CDRs include the duration, source number, and name of the upstream provider for each call. Through the CDRs, providers can distinguish between legal and illegal robocalls by examining the percentage of calls answered, the ratio of different caller ID information displayed (referred to as Automated Numbering Information, or ANI) to the number of total calls, the average duration of calls, and the percentage of calls of less than one minute.<sup>99</sup> These behaviors will show clear indications of fraud.



TABLE 6  
**Comparing Legal Robocalls to *Illegal* Robocalls**<sup>100</sup>

LEGAL ROBOCALLS	ILLEGAL ROBOCALLS
Relatively high percentage of calls are answered	Low percentage of calls are answered
Legitimate telemarketer typically uses only a single caller ID for the entire telemarketing campaign or demographic. (This allows callers to track their calls)	Spoofed caller IDs, with caller ID-to-called-number ratios often fewer than 2 (meaning that each caller ID is used for 2 or fewer calls)
	Almost all calls are short duration, <ul style="list-style-type: none"> <li>■ averaging less than 20 seconds (because the called party hangs up or sends to voicemail)</li> <li>■ 99% or more of calls last less than a minute</li> <li>■ Fewer than 1% of calls last more than 2 minutes</li> </ul>

The recently filed case by the North Carolina Attorney General against provider Articul8 provides a concrete example of how these metrics can be used to determine illegal calls. According to the complaint, in a single day Articul8 routed through a downstream (intermediate) provider over 17 million calls, more than 70% of which were not answered. Of the 4.4 million calls that were answered the average duration was 11 seconds. The call-per-ANI ratio was 1.08, meaning nearly each of the more than four million calls seemed to come from a distinct (illegally spoofed) number.<sup>101</sup>

With these hallmarks of fraud, the information in the CDRs is clear indication that the calls are illegal robocalls. And reviews of their own CDRs inform responsible providers of the type of traffic they are transmitting.<sup>102</sup> Indeed, responsible providers review their CDRs regularly to ensure that they are not transmitting illegal calls and to terminate relationships with upstream providers whose calls bear indications of fraud.<sup>103</sup>

However, as CDRs are also proof of illegal traffic, some providers seek to eliminate that proof by destroying their CDRs and those of their downstream providers. Indeed, in its recent complaint, the Vermont Attorney General alleges that the defendant was “deliberately” destroying these records.<sup>104</sup>

**Content Analytics.** Providers can confirm suspected illegal robocall traffic by using “content analytics.”<sup>105</sup> As a way to control the torrent of unwanted calls, YouMail, and other service providers to the telephone industry, have been given access by their customers to their voicemail. Other service providers have their own “honey-pots” (telephone numbers owned by the recipient to monitor patterns of illegal calls) to capture information about illegal calls. Recordings of the scam calls are captured on these millions of voice mailboxes, which then enable the providers to determine the true intent of these calls through the words used in the message left on the voicemail.<sup>106</sup> Using this “content analytics” method, these providers are then able to block the transmittal of similar calls deemed to be illegal.<sup>107</sup>

One provider blocking illegal calls will not resolve the problem, as scam callers will simply find another call path to reach vulnerable Americans' phones (and their pockets). Unless all U.S. providers implement appropriate blocking protocols, scammers will still be able to find a way to defraud American phone subscribers.

Because voice service providers make money from connecting calls, whether those calls are legitimate or not, voice service providers are incentivized to look the other way and accept payment for permitting illegal traffic to reach American phones. That incentive structure needs to change. In September 2021, FCC Commissioner Geoffrey Starks noted this counterproductive dynamic regarding robocalls: “[I]llegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it. Last year’s estimated 46 billion robocalls and last month’s estimated 4.1 billion calls are proof positive of that.”<sup>108</sup>

As described in Section IV, the FCC has not yet taken effective action to stop these scam robocalls. Unfortunately, the providers complicit with the scam robocallers will continue to dump scam traffic into the American phone system so long as it is profitable for them to do so.

#### *E. Providers have a system to filter out some spam texts, but it is insufficient.*

As explained in Section II, the number of scam texts is also increasing. This is so despite the voluntary registry established by the major cell phone providers. Senders who join the registry must abide by registry rules, such as allowing the registry to categorize the type of sender and the content of the messages, and requiring registry texts to contain a “stop” mechanism, which informs recipients that they can request that texts from that text sender no longer be sent.<sup>109</sup> In return for using the registry for text campaigns,<sup>110</sup> text senders are charged less for registry-compliant messages than text campaigns that are not sent through the registry.<sup>111</sup> By offering discounted prices for texts sent in compliance with their rules,<sup>112</sup> the registry gives an incentive to text senders to use the registry. The registry blocks texts sent through the registry that are patently fraudulent.

However, the use of the registry is voluntary, and its rules apply only to texts sent through the registry. There is no rule or mechanism that requires participation in the registry or prevents automated text messages from being sent without being submitted to the registry. Text scammers have no reason to follow these registry rules.

## IV. THE U.S. GOVERNMENT HAS NOT BEEN ABLE TO STOP THE SCAM CALLS.

The goal of the Telephone Consumer Protection Act, passed by Congress in 1991, was to give telephone users some control over automated calls.<sup>113</sup> Yet, as virtually every telephone subscriber in 2022 knows, the problem of unwanted calls has continued to escalate.

In a further effort to address illegal robocalls as well as the mushrooming problem of callers using fake caller IDs (referred to as spoofing), Congress passed the TRACED Act in 2019.<sup>114</sup> Since then, the FCC has adopted several regulations and is proposing additional initiatives to combat fraudulent calls. However, despite these efforts, in each of the past two years more than **20 billion scam robocalls** were made to U.S. telephone subscribers.<sup>115</sup>

### *A. The Federal Communications Commission's (FCC's) approach to regulating robocalls has not solved the problem.*

This is in no small part due to the Commission's approach to regulating robocalls—for more than two years, the Commission has made it clear that it expects providers to couple STIR/SHAKEN (or other “reasonable measures” of call authentication) with reasonable use of call analytics, and that providers are permitted (but not required) to block calls likely to be illegal.<sup>116</sup> In so doing, the Commission has placed the emphasis on reasonableness and provider discretion, rather than on effectiveness at actually stopping robocalls.

Unfortunately, while the FCC has initiated numerous proceedings to deal with illegal robocalls, we believe that none of these, either singly or in combination, will effectively stop most of the illegal calls, for these reasons:

- Requiring STIR/SHAKEN attestation only requires telecommunications providers to assess the reliability of the caller IDs attached to calls. Even full compliance will not stop the scam callers.
- No existing or proposed rule or policy requires all providers to act affirmatively to stop criminal robocalls; providers are permitted to wait for the FCC to tell them to take action.
- Existing and proposed regulations designed to prevent illegal robocalls generally consider providers to be compliant if they have a policy or procedure in place, rather than measuring compliance based on results.
- There is no automatic mechanism for suspending noncompliant providers from the network, and no limitation preventing individuals who have processed criminal robocalls in the past from simply creating a new company under a different name and continuing to transmit illegal calls.

- The powerful Traceback tool is not being utilized effectively.

As this report went to print, the FCC announced a vote on new regulations and proposed regulations for Gateway Providers.<sup>117</sup> Our preliminary evaluation suggests that this order largely represents more of the same approach from the FCC. As such, all of our concerns will likely remain, however that will depend on what the FCC ultimately issues in its final orders.

**1. The FCC permits but does not require providers to block illegal calls.** In 2017, the FCC clarified that voice service providers were permitted to block calls considered “highly likely to be illegal” because they appeared to be from numbers that were not in use.<sup>118</sup> This permission was extended in 2020 to allow providers to use “reasonable analytics to provide network-based blocking” of calls “highly likely to be illegal.”<sup>119</sup> Neither of these measures *requires* providers to block these calls. Since providers are paid per answered call that they transmit,<sup>120</sup> it should not be a surprise that giving them permission to block calls has not been effective these past five years. The enormous numbers of fraudulent calls that continue to reach American consumers shows that providers need to be required to identify and block illegal calls.

**2. Addressing caller-ID spoofing will not stop scam robocalls.** The TRACED Act required the FCC to implement the STIR/SHAKEN methodology to authenticate caller IDs associated with robocalls.<sup>121</sup> Implementation has been mandated for most of the industry and will certainly help reduce telemarketers’ use of spoofed caller IDs. However, applying the STIR/SHAKEN methodology is unlikely to cause a significant decrease in scam robocalls.

STIR/SHAKEN requires only that originating providers apply a certification to each call that indicates how confident the provider is that the caller ID accompanying the call is correct.<sup>122</sup> An originating provider is considered to be in full compliance with STIR/SHAKEN even when it merely gives calls a B level attestation (indicating that the provider is not sure), or a C level attestation (indicating that it has no ability to authenticate the source of the call).<sup>123</sup> Those attestations do little to ensure that the caller IDs accompanying the calls are truthful.<sup>124</sup>

More fundamentally, complying with STIR/SHAKEN only establishes that the caller ID is not spoofed. As long as telecommunications providers are allowed to rent rotating series of numbers to their customers making illegal calls, the caller ID may be truthful, since the caller has the right to use the rented numbers when the calls are made, but the ID information itself will be meaningless. As the telephone number identified is only fleetingly associated with the caller, it does not provide an effective way to identify the caller or even block the caller’s calls.

**3. The Robocall Mitigation Database does not stop scam robocalls.** As of June 30, 2021, originating voice service providers must certify in the newly created Robocall Mitigation Database (RMD) that they have implemented STIR/SHAKEN for that part of their networks that use internet protocols.<sup>125</sup> Providers that do not use the internet to transmit calls must have alternative robocall mitigation plans.<sup>126</sup> And some small providers have been granted an extension until June 30, 2022 to comply with STIR/SHAKEN,<sup>127</sup> as long as they certify in the RMD that they are employing an alternative robocall mitigation program. Effective September 28, 2021, the FCC prohibits intermediate and terminating providers from accepting telephone traffic directly from any providers not listed in the RMD.<sup>128</sup>

An access barrier like the RMD could be a powerful tool to stop scam calls. However, for reasons described in #2, *supra*, its focus on compliance with STIR/SHAKEN means that the RMD will not stop scam calls. Moreover, there is no requirement, much less an automated mechanism, that non-compliant providers be suspended from the RMD,<sup>129</sup> and the FCC does not have the scale to monitor compliance by each of the 4,000 providers that have registered.

In addition, because there are such low entry requirements for setting up business as a VoIP provider, there is no meaningful barrier to stop providers who have been caught from simply setting up shop using a different name and continuing with the same illegal behavior.<sup>130</sup> Any provider anywhere in the world can create an entry in the RMD by filling in a form and clicking a few boxes. As a result, in its current configuration the RMD is of limited use in ensuring compliance even with the STIR/SHAKEN protocol, let alone with engaging in effective robocall mitigation.

**4. The powerful potential of ITG Tracebacks is underutilized.** Pursuant to the direction in the TRACED Act the FCC selected USTelecom (a trade association for telephone companies and providers of broadband service) to conduct tracebacks of suspected unlawful robocalls.<sup>131</sup> As described in Section III D, *supra*, the ITG traces suspicious traffic from the terminating provider back through intermediate providers to the gateway or originating provider and then to the caller, when the originating provider provides that information in the traceback.<sup>132</sup> Each provider in the call path is notified that the call being traced was illegal and each provider is generally given the content of the illegal call. However, although the ITG *may* refer the information from tracebacks to state or federal enforcement authorities, there is no requirement that it does so.<sup>133</sup>

The ITG conducted more than 5,400 tracebacks in 2020 and 2021.<sup>134</sup> However, the details about these tracebacks are not disclosed. If revealed, this traceback work could have a profound effect on stopping illegal calls, but its potential is not being used. First, information about completed tracebacks would have enormous



value to providers seeking to avoid transmitting scam calls, as it would enable them to identify and avoid accepting calls from the gateway, originating, and intermediate providers that have been found in previous tracebacks to have repeatedly transmitted these calls. Making traceback requests public would also enable attorneys general and scam victims to identify complicit providers and hold them liable. All these steps would place market pressure on originators and facilitators of scam calls. Yet nearly all the information regarding tracebacks is currently secret, available only to the ITG itself and provided to the FCC, the FTC or state AGs based on non-public rules.

The FCC does include information about tracebacks in its annual report to Congress. This report is of little use to providers and others in identifying entities to which fraudulent calls have been repeatedly traced, however, because it does not distinguish problematic providers from cooperative providers. The Commission reports providers as either participating in traceback; being non-responsive to one or more tracebacks; or being non-responsive to three or more consecutive tracebacks. But merely responding to traceback requests does not show providers are complicit in transmitting illegal calls, as traceback requests typically start with the terminating provider that transmitted the call to the called party, which usually occurs after the illegal calls have been so mixed in with legitimate calls that they cannot be identified. As a result, the Commission's 2020 and 2021 reports to Congress present providers such as thinQ,<sup>135</sup> RSCoM,<sup>136</sup> Piratel,<sup>137</sup> and Globex<sup>138</sup> that have been defendants or respondents in enforcement actions as being just as cooperative as the likes of Verizon and AT&T.<sup>139</sup>

Second, there is insufficient follow-up on tracebacks by enforcement authorities. Once the ITG has completed a traceback of a suspected illegal call, it is allowed to but not required to refer the information to state or federal enforcement authorities.<sup>140</sup> Even though ITG conducted more than 5,400 tracebacks in 2020 and 2021<sup>141</sup>—many against the same providers—the FCC sent only 18 cease and desist letters between January 1, 2021 and April 1, 2022.<sup>142</sup> The FCC has not sent any cease and desist letters against Articul8, the defendant in the case brought by the North Carolina Attorney General, even though Articul8 had 49 tracebacks.<sup>143</sup> The FCC sent a cease and desist letter to TCA VoIP, the defendant in the Vermont Attorney General's case, only a few weeks before that case was filed, even though TCA VoIP had been the recipient of 132 tracebacks over a period of two years.<sup>144</sup> In addition, while the TCPA regulations were amended in 2021 to require voice service providers to respond to tracebacks,<sup>145</sup> there is no provision for automatically suspending those who do not comply from the Robocall Mitigation Database.

**5. The requirement that originating providers “Know Your Customer” does not stop the illegal calls.** Both Congress and the FCC have recognized that the “rising tide of robocalls and the emergence of VoIP go hand in hand.”<sup>146</sup> Section 6 of the TRACED Act required the FCC to initiate proceedings to require VoIP providers to “know their customers.”<sup>147</sup>

In 2021, the FCC amended its regulations to add a requirement that each voice service provider “[t]ake affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls, including knowing its customers and exercising due diligence in ensuring that its services are not used to originate illegal traffic.”<sup>148</sup> However, in its May 2022 order, the FCC may impose additional requirements for providers to describe how they will “know” their upstream providers (see # 6 *infra*).

This requirement is a good start, but it has significant loopholes. First, it appears to apply only to providers whose customers “originate” calls, so is not clearly applicable to gateway providers that transmit calls from abroad, or to intermediate providers that accept calls from either originating, gateway or other intermediate providers. Second, it does not include a clear rule requiring that downstream intermediate providers or terminating providers that are capable of identifying suspicious traffic block illegal calls from reaching their customers. In addition, the FCC has not brought any action to date for violating these requirements, nor has it articulated a clear enforcement mechanism.

**6. The pending proceedings for problematic VoIP providers and gateway providers would only require certifications and policies.** As of April 2022, the FCC has initiated two additional proceedings to address illegal robocalls. In the first, recognizing that the illegal problem calls are typically made through small VoIP providers, the FCC has proposed that VoIP providers be required to certify “that the provider will not assist and facilitate illegal robocalling, illegal spoofing, or fraud, and that it will take reasonable steps to cease origination, termination, and/or transmission of illegal robocall traffic once discovered.”<sup>149</sup> The proposal also would require VoIP providers to “certify that its traffic is signed with STIR/SHAKEN or is subject to a robocall mitigation program in order to file in the Robocall Mitigation Database.”<sup>150</sup> However, this proposal does not include any mechanism for suspending a provider from the RMD that has been determined to have a) transmitted illegal calls, b) certified its traffic incorrectly, or even c) failed to respond to traceback requests. Additionally, it requires “reasonable steps” rather than “effective measures,” meaning that providers are off the hook if they have procedures designed to address robocalls, regardless of whether their efforts are actually effective in reducing robocalls.

In the second proceeding relating to gateway providers, the FCC requested comments on how to prevent foreign-originated illegal robocalls from entering

the American telephone network through gateway providers.<sup>151</sup> The Commission proposed a myriad of potential steps that gateway providers could be required to take to limit the flood of illegal calls from abroad. But, even if the steps all are ordered, the regulatory structure would still seem to allow providers to evade the consequences of transmitting illegal calls so long as the providers had “policies and procedures” designed to avoid transmission of calls, instead of simply requiring that providers ensure that they do not transmit illegal calls. Additionally, providers downstream from the gateway providers would be permitted to delay blocking bad-actor gateway providers until receiving notification from the Commission.<sup>152</sup>

**7. Proposed Limitation of Access to Numbers by VoIPs.** Currently, VoIP providers are permitted access to large numbers of telephone numbers which they can rent to their caller-customers to use on a rotating basis.<sup>153</sup> Callers can then rotate through these rented numbers to make only a few calls using each number. This allows these illegal calls to evade the analytics applied by downstream providers attempting to identify—and then block—illegal robocalls. (Some complicit VoIP providers even advertise access to this system to attract illegal callers.<sup>154</sup>) As there is no good reason for this proliferation of numbers, the FCC is considering how VoIP providers should be limited to direct access to telephone numbers, as required by Section 6 of the TRACED Act.<sup>155</sup>

Unfortunately, the FCC only proposes to require the VoIP providers to certify that they will use numbering resources lawfully, and to describe in the RMD their steps to ensure compliance.<sup>156</sup> Requiring the very VoIPs that have been deliberately facilitating illegal calls to American subscribers to adopt procedures and make a promise that they will operate “lawfully” seems like an exercise in futility. It would be much more effective to require all originating and intermediate VoIPs to monitor their traffic, and then to require that access to the network be terminated for any providers found to be transmitting illegal calls.<sup>157</sup>

**8. The FCC’s enforcement actions have not been sufficient to stop or slow the scam calls.** The FCC’s enforcement efforts consist largely of sending cease and desist letters to providers that have been determined through the traceback process to have repeatedly made illegal calls, and six enforcement actions.<sup>158</sup> But of the more than 5,400 tracebacks ITG conducted in 2020 and 2021<sup>159</sup>—many against the same providers—as of the time of this writing, the FCC has announced only 18 cease and desist letters since January 2021.<sup>160</sup>

Another weakness is that, even when a particular provider has been the respondent in an enforcement effort brought by the FCC—such as John Spiller was in 2020<sup>161</sup>—there is currently nothing to stop that provider from recasting itself under a different name and resuming its illegal business practices. Indeed, this seems to be exactly what was done by John Spiller, who faced the FCC’s

largest fine of \$225 million, did not pay it, and apparently continued in the same business.<sup>162</sup> The ease of re-registering in the RMD creates the concern that fraudulent callers will still be able to use this revolving door tactic.

Moreover, these enforcement methods are all reactive rather than proactive. They are brought only *after* the billions of calls were made, the privacy of tens of millions of subscribers has been violated, and millions of consumers have lost money to the scams perpetrated in the robocalls. Instead of relying on after-the-fact cease-and-desist orders and forfeitures, little of which is ever collected, the FCC should require all providers in the call path to proactively employ analytics and other tools to identify illegal calls, and then refuse to transmit them. This more proactive approach would protect not only consumers, but would also benefit legal robocallers, whose calls will be less likely to be improperly labeled or blocked.

### ***B. The Federal Trade Commission's (FTC's) enforcement of the Telemarketing Sales Rule (TSR) is unlikely to stop the illegal calls.***

The Telemarketing Sales Rule prohibiting deceptive and abusive telemarketing acts and practices,<sup>163</sup> issued by the Federal Trade Commission, declares it a deceptive act for a person to provide substantial assistance to a telemarketer while knowing, or consciously avoiding knowledge, that the telemarketer is violating the TSR.<sup>164</sup> An individual or company that provides substantial assistance can be held liable for a TSR violation even without meeting the definition of “seller” or “telemarketer,”<sup>165</sup> so a VoIP provider that knows or consciously avoids knowing that the calls it transmits are fraudulent can be held liable under this standard.

The FTC has been using its authority under the TSR to investigate and punish VoIP providers that have transmitted millions of illegal robocalls. It has issued several civil investigative demands against VoIP providers,<sup>166</sup> and successfully sued other VoIP providers, resulting in substantial fines and lifetime bans from engaging in the business.<sup>167</sup> The FTC also issued 19 warning letters in early 2020 to VoIP providers.<sup>168</sup> Unfortunately, the FTC's actions to date have not created sufficient incentives among VoIP providers to stop the transmittal of illegal robocalls. As this report went to print, the FTC voted on new proposed regulations for telemarketers, including record-keeping requirements, and extending the protection of the TSR in the realm of business to business (B2B) telemarketing and inbound calling.<sup>169</sup> While these measures will bolster enforcement of the TSR, they are unlikely to stop the calls from coming in the first place because not all providers are adequately incentivized to stop accepting illegal traffic.

## V. THE FCC CAN STOP MOST SCAM ROBOCALLS AND ILLEGAL TEXTS—HERE IS HOW.

Every month in which the issue of scam robocalls is not meaningfully resolved, more than one billion more scam calls assault American subscribers, and millions lose money to those scams. The current system protects providers, rather than ensuring the protection of the American subscribers from fraudulent robocalls.

These scam robocalls are transmitted as the result of the choices made by service providers regarding what calls they accept payment for transmitting. The originating provider makes a choice to accept calls from a certain robocaller and sends those calls to an intermediate provider who chooses to accept and transmit those calls down the call path. If that first intermediate provider decides not to accept the calls from the originating provider, the scam calls are stopped at that point and do not reach the called party unless the originating provider finds another intermediate provider willing to take them. Similarly, each hop in the chain to a subsequent intermediate provider or the terminating provider represents a separate decision by the downstream provider to accept and transmit those calls or to block them. Currently, the primary determinant for many of these instantaneous decisions made by the providers in the call path is profit. That must change.

We propose that, to stop the criminal robocalls, three principles must be paramount:

1. All providers in the call path should have an affirmative obligation to engage in effective mitigation against illegal robocalls.
2. Providers who knew or should have known that they were transmitting illegal robocalls should face clear financial consequences.<sup>170</sup>
3. Law enforcement, telephone service providers, victims of scam calls, legal robocallers, and the general public should have access to all available information about the sources of the illegal robocalls and their complicit providers.

Much of what we say in the five proposals below is supported by various arms of the telecom industry, and state regulators.<sup>171</sup>

### **Proposal 1: Require that all providers in the call path engage in effective mitigation against illegal robocalls.**

Current FCC rules only *permit* intermediate providers to stop scam calls, rather than require them to do so.<sup>172</sup> Likewise, terminating providers are permitted, rather than required, to block calls when analytics indicate that the calls are likely illegal.<sup>173</sup> Providers are only required to “effectively mitigate illegal traffic when

[they] receive actual written notice of such traffic from the Commission. . . .”<sup>174</sup> Originating providers—and now—gateway providers are required to take “effective measures” to prevent their customers from using their networks to transmit illegal calls. However, gateway providers are still not required to block illegal calls (except those on a “Do Not Originate” list) until notified by the Commission to do so.”<sup>175</sup>

*The FCC regulations should be changed to require that all providers, including intermediate providers, use all available methodologies and block scam calls as soon as they are discovered.*

Intermediate providers, especially those in upstream positions that accept calls directly from originating or gateway providers, are often in the best position to recognize and block illegal calls. They should be required to do so.

Terminating providers may be less able to block individual calls on the basis of behavioral analytics because they receive so many calls from intermediate providers who are far down the call path from the initial intermediate providers (those accepting calls from the originating providers). But terminating providers have the power to require that their directly upstream intermediate providers not accept illegal calls from their respective (further) upstream providers. The upstream providers, using either traceback information or content or behavioral analytics, can more easily block fraudulent calls.

The terminating providers can protect themselves, for example, by requiring that the upstream providers sending them calls impose the same mandate on their upstream providers. In this way, the marketplace can impose the same conditions all the way upstream to the originating or gateway providers. The FCC should structure the blocking requirements so that providers are either required to, or have strong incentives to, refuse to accept future calls from upstream providers that have transmitted scam calls, as indicated by tracebacks or call or traffic analytics.

**Proposal 2: Clear financial consequences should apply to providers who transmit illegal robocalls when they knew or should have known that the calls were illegal.**

As described in Section III there are tools currently available that allow providers to identify and then block scam robocalls. But providers need to be incentivized to use these tools and to block the calls found to be illegal. As described by one FCC Commissioner, “illegal robocalls will continue so long as those initiating and facilitating them can get away with and profit from it.”<sup>176</sup>

The choices that providers in the call path make about whether to accept calls from upstream providers should be guided not only by the price paid for those calls, but also by the risk involved in accepting calls from those upstream providers. The consequences of the wrong choice should be steep.



The Fair Credit Billing Act (FCBA),<sup>177</sup> which governs the relationship between banks and consumers who use credit cards, illustrates why placing the financial liability on providers for illegal calls will be an effective mechanism to stop scam robocalls. The FCBA imposes the cost of losses from credit card fraud and error on the banks, rather than consumers. As a result, the banking industry has developed a robust set of protections governing the use of credit cards to minimize their own losses from theft, fraud and even user negligence. The banks control the system, imposing on merchants their requirements to protect against losses. While there are extensive regulations issued by federal regulators that govern the transactions between the banks and their customers (e.g., disclosures and rules governing imposition of finance charges), there are no rules governing *how* the banks should protect themselves from losses caused by fraudsters. The banks—which will bear the burden of failure—have every incentive to develop vigorous procedures to limit these losses. The security procedures used by banks to monitor and avoid losses is constantly changing, to combat new threats.

The telephone service providers should be similarly incentivized to develop and use procedures to guard against transmitting fraud robocalls.

*The rules should clearly state that all providers in the call path of a fraudulent call are liable for the consequences of that call if the provider knew or should have known that the call was illegal. Pursuant to Proposal 1, this would apply to nearly all illegal calls, as all providers in the call path would be required to use every available mitigation tool to determine the illegality of the calls, and then block them.*

We do not recommend that the FCC prescribe the specific methods of implementation necessary to stop the transmission of illegal robocalls effectively. Just as the FCBA does not tell banking institutions how to prevent frauds and other losses, the FCC's rules should simply provide the incentive for the telephone service providers to find and use every available, reasonable method of detecting and blocking the illegal calls. But to illustrate how this might work, we offer suggestions and examples of how providers might achieve this.

For originating, gateway, and first intermediate providers specifically, there is little excuse for continuing to transmit scam robocall traffic after any notice that the traffic is illegal based on previous tracebacks or FCC cease and desist letters. But these providers also must be incentivized to employ additional tools, such as behavioral analytics (e.g. the patterns of the calls sent from that provider, such as the duration of the calls, and the number of different caller IDs used, etc.), and to analyze the content of the calls (capturing and reviewing the messages in the robocalls).<sup>178</sup> Additionally, contracts between providers should require that calls from upstream providers will stop being accepted if, for example, the upstream provider has a history of transmitting illegal calls, fails to respond to tracebacks,

or other analytics indicate that calls from the provider are likely illegal. Providers who do not include and enforce such terms in their contracts should be held liable for the fraud losses suffered by consumers.<sup>179</sup>

Requiring bonds for providers (see Proposal 5, *infra*) can also address concerns regarding providers who might not have sufficient financial capital to compensate consumers for their losses.

**Proposal 3: The FCC should use suspension<sup>180</sup> from the Robocall Mitigation Database as a mechanism to protect telephone subscribers from receiving illegal calls, pending investigations. This would place a higher priority on protecting U.S. telephone subscribers from criminal scam calls and texts, than on providing VoIP originating and gateway providers access to the U.S. telephone network.** To accomplish this, we recommend the following possible triggers for suspension:

- a. The provider knows, or consciously avoids knowing, that it has transmitted illegal calls into the U.S. telephone network, subject to appropriate safe harbors established by the FCC;
- b. The ITG has conducted a subsequent traceback that identifies a VoIP provider that had previously either (i) originated criminally fraudulent calls to American telephone numbers or provided gateway services to callers making such calls, or (ii) been the first intermediate provider of services to the originating or gateway provider described in subsection (i);
- c. The provider fails to respond to a traceback request with 48 business hours from a request from the ITG;<sup>181</sup> or
- d. The provider is determined to be owned or operated by any individuals who owned or operated VoIP providers previously punished or sanctioned by the FCC, or any other federal or state law enforcement agency, for providing service to callers making illegal calls.

Safe harbors might be permitted for terminating and downstream providers who are unable to block individual scam robocalls because of the way in which the calls are delivered to them, so long as these providers are otherwise engaged in effective mitigation.<sup>182</sup>

**Proposal 4: All tracebacks conducted by the ITG should be made public.** Making tracebacks public will enable providers throughout the call path to identify the sources of illegal calls and use their market power to prevent those calls from reaching subscribers.<sup>183</sup>

Legal robocallers will also benefit if tracebacks are made public. They will be able to require that their originating providers not transmit calls through any intermediate providers that have been repeated recipients of tracebacks.

These legal robocallers will be empowered to protect their calls from being inappropriately blocked or misidentified because their calls were transmitted through providers that had a history of transmitting illegal calls.

To accomplish this, the FCC should require that all tracebacks conducted by the ITG be made public within 24 hours of the traceback. To ensure the privacy of the subscribers receiving the calls, the last four digits of the subscriber's telephone number in each traceback should be redacted.

**Proposal 5: The FCC should impose (or be empowered to impose) strict licensing and high bonding requirements for VoIP providers, subject to an exception for providers with a strong history of compliance.** To accomplish this, the FCC should require that VoIP providers:

- a. Submit to the Commission an application for a license, or a renewal of an existing license, that includes the names and contact information of the individuals who own the provider or, if the provider is a corporation, the majority shareholders of the corporation and other parties of interest with respect to the management of the provider, as determined appropriate by the Commission to ensure that persons with a history of transmitting calls in violation of this section are ineligible for such a license;
- b. Provide to the Commission evidence that the provider has posted a surety bond of \$1,000,000, or such additional amount that the Commission may require based on the provider's record of transmitting illegal calls.

The scourge of scam robocalls and texts is responsible for more than one billion illegal calls every month—while merely annoying to some, to many vulnerable Americans these scam messages are ruinous. Although the FTC, the FCC, and some telecom companies have undertaken extensive efforts to remedy the problem, we are not optimistic that they will achieve their purported goal unless: providers are required to employ effective mitigation strategies (not merely “reasonable steps”), and providers are financially punished when those strategies fail to protect consumers from scam messages. Finally, to maximize swift and effective measures to protect consumers, information about tracebacks and other determinations that providers are transmitting illegal robocalls should be made public.

## ENDNOTES

1. See 47 U.S.C. § 227(a). [Federal Trade Comm'n, Consumer Advice, Robocalls](#) (“If you answer the phone and hear a recorded message instead of a live person, it’s a robocall.”).
2. 47 U.S.C. § 227. The TCPA also makes it illegal to use an automated telephone dialing system (ATDS or autodialer) to call a phone subscriber without first obtaining consent, with a few exceptions.
3. 47 U.S.C. § 227(b)(1).
4. Americans are losing significant amounts to *live* scam calls as well. However, those live calls are beyond the scope of this report. See, e.g., Public Service Announcement, Federal Bureau of Investigation, [FBI Warns of the Impersonation of Law Enforcement and Government Officials](#) (Mar. 7, 2022).
5. According to estimates from YouMail, since 2018, no fewer than 45.87 billion robocalls have been sent to American phones in a calendar year, with no fewer than 37% and as many as 46% of these calls representing scam robocalls. Dividing this minimum annual number by 12 to approximate a monthly average, and assuming the minimum estimated percentage of 37%, our conservative estimate is that more than 1.4 billion scam robocalls are made to American phones every month. YouMail estimates that there were 47,839,232,200 placed in 2018, 58,536,224,700 placed in 2019, 45,866,949,500 placed in 2020, and 50,507,702,500 placed in 2021. YouMail, [Historical Robocalls By Time](#). YouMail estimates that 37% of robocalls placed in 2018 were scam robocalls. PR Newswire, [Nearly 48 Billion Robocalls Made in 2018, According to YouMail Robocall Index](#) (Jan. 23, 2019). YouMail estimates that 44% of robocalls placed in 2019 were scam robocalls. PR Newswire, [Americans Hit by Over 58 Billion Robocalls in 2019, Says YouMail Robocall Index](#) (Jan. 15, 2020). YouMail estimates that 46% of robocalls in 2020 were scam robocalls. PR Newswire, [Americans Hit by Just Under 46 Billion Robocalls in 2020, Says YouMail Robocall Index](#) (Jan. 26, 2021). YouMail estimates that 42% of robocalls in 2021 were scam robocalls. PR Newswire, [U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#) (Jan. 6, 2022).
6. See *id.*
7. YouMail confidential data provided to NCLC [hereinafter YouMail Data Provided to NCLC]. After identifying the top 1,000 scam campaigns in a single month and examining the calls made in January 2022 by only those top campaigns, YouMail indicated in its private data that more than 458 million scam robocalls were made by the top 1,000 scam robocall campaigns in that 30-day period.
8. Frank Green, [Chesterfield woman’s life is upended in \\$10 million robocall scam](#), Richmond Times-Dispatch, June 10, 2021. [Another example of this type of call is available here.](#)
9. There were over 8.6 million of these types of calls made in January 2022. YouMail Data Provided to NCLC, *supra* note 7.
10. This number is reached by combining fraud reported by age 60-69, 70-79, and 80+ (521MM+364MM+149MM = 1.034BB). See FTC Consumer Sentinel Network, [Reported Frauds and Losses by Age, Year: 2021](#) (updated Feb. 22, 2022) (Age & Fraud tab, Year 2021, with quarters 1 through 4 checked).
11. Stephen Nessen, NPR, [Chinese Robocalls Bombarding the US Are Part of an International Phone Scam](#) (May 10, 2018).
12. YouMail estimates that in January 2022 there were over 12.3 million disability benefits scam robocalls. YouMail Data Provided to NCLC, *supra* note 7. [A typical recording is available here.](#)

13. YouMail estimates that in January 2022 there were over 32.6 million student loan scam robocalls. YouMail Data Provided to NCLC, *supra* note 7. [A typical recording is available here.](#)
14. YouMail estimates that over **114 million of these scam robocalls** caused U.S. telephones to ring in January 2022. YouMail Data Provided to NCLC, *supra* note 7. [A recording of a sample call is available here.](#)
15. YouMail estimates that over **25.6 million of these Medicare scam robocalls** rang on subscribers' phones in January 2022. YouMail Data Provided to NCLC, *supra* note 7. [A recording of a sample call is available here.](#)
16. YouMail estimates that over 70 million health insurance scam robocalls rang on subscribers' phones in January 2022. YouMail Data Provided to NCLC, *supra* note 7. [A recording of just one of many health insurance campaign scam calls is available here.](#)
17. YouMail estimates that over 15.8 million bill reduction scam robocalls rang on subscribers' phones in January 2022. YouMail Data Provided to NCLC, *supra* note 7. [A recording of just one of many fake bill reduction campaign calls is available here.](#)
18. YouMail estimates that over 140,000 IRS scam robocalls rang on subscribers' phones in January 2022. YouMail Data Provided to NCLC, *supra* note 7. See Courier Video, [Fake IRS Scam Recording](#), YouTube (Jul. 2, 2017) (last visited Feb. 10, 2022).
19. YouMail estimates that over 19.5 million business impersonation scam robocalls rang on subscribers' phones in January 2022, with more than 13.7 million scam robocalls relating explicitly to Amazon (including fake fraud alert and automatic charge scams). YouMail Data Provided to NCLC, *supra* note 7. [A recording of a sample call is available here.](#) See also Hiya, [State of the Call 2022 Report 7](#) (2022) (noting that 62% of phone subscribers surveyed reported having received a business impersonation scam call in 2021). The FTC reported consumer financial losses from business impersonation scams (by any contact method, not just phone) more than tripled between 2019 and 2021, exceeding \$451 million in 2021 alone. Press Release, Federal Trade Comm'n, [FTC Outlines Aggressive Approach to Policing Against Pandemic Predators in Testimony Before Senate Commerce Subcommittee](#) (Feb. 1, 2022). Regarding Amazon impersonations specifically, the FTC reported that more than one in three complaints (36%) about business impersonation scams in the twelve-month period preceding July 2021 were from scammers claiming to be Amazon. Emma Fletcher, Federal Trade Comm'n Data Spotlight, [Amazon tops list of impersonated businesses](#) (Oct. 20, 2021) (6% of scammers claimed to be Apple).
20. The robocall blocking company YouMail has thousands of recordings of such fraud campaigns.
21. See Federal Commc'ns Comm'n, [Caller ID Spoofing](#).
22. This is called "neighbor spoofing." See Better Business Bureau, BBB Scam Alert: ["Neighbor spoofing" is a common type of phone scam](#) (May 29, 2020).
23. See YouMail, What Everyone Needs to Know about Leased Telephone Numbers and Unwanted Robocalls, presentation at SIPNOC 2022 Webinar Series (Mar. 21, 2022) [hereinafter What Everyone Needs to Know]. See also *In re Call Authentication Trust Anchor*, [Second Report and Order](#), WC Docket No. 17-97, at ¶ 50 (Rel. Oct. 1, 2020), [hereinafter Oct. 1, 2020 Second Report and Order] (noting that some providers lease numbers and do not have direct access to numbering resources).
24. See FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amounts by Contact Method](#) (updated Feb. 22, 2022) (Losses & Contact Method tab, with quarters 1 through 4 checked for 2021 and 2020; indicating 644,048 fraud reports using the phone call contact method and 377,840 using the text contact method from Q1-Q4 2021, as compared with 382,036 phone call and 334,952 text fraud reports for Q1-Q4 2020).



25. The 60% figure is consistent with Truecaller data. Truecaller, [Truecaller Insights 2021 U.S. Spam and Scam Report](#) (June 28, 2021) [hereinafter Truecaller Insights]. By quoting Truecaller's statistics, we are not endorsing Truecaller's business model, as we are aware of concerns that have been raised. See, e.g., Alfred Ng, CNET, [Those robocall blocker apps are hanging up on your privacy](#) (Aug. 10, 2019); Rest of World, [How Truecaller built a billion-dollar caller ID data empire in India](#) (Mar. 2022).
26. In calculating this figure, we assumed that 100% of scam texts were automated, but, consistent with Truecaller's estimate, that only 60% of the scam calls were robocalls.
27. FTC Consumer Sentinel Network, Fraud Reports by Contact Method, [Reports & Amount Lost by Contact Method](#) (updated Feb. 22, 2022) (Losses & Contact Method tab, with quarters 1 through 4 checked for years 2017 through 2021).
28. Truecaller Insights, *supra* note 25 (reporting on results of Harris Poll surveys). Truecaller's data includes scam calls reported as robocalls, as well as calls that were not identified as robocalls, although many calls that appear to be live calls are likely calls made with prerecorded voices and artificial intelligence, which are in fact robocalls. See Appendix 1, *infra*.
29. Truecaller Insights, *supra* note 25.
30. This figure represents an increase of greater than 50% from \$19.7 billion in 2020. Truecaller Insights, *supra* note 25.
31. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amounts Lost by Contact Method, Year: 2021](#) (updated Feb. 22, 2022). Note that this figure captures consumer complaints for all scam calls, not just those scam calls reported as robocalls, and that it likely understates the magnitude of the problem, as only a small percentage of consumers go through the trouble of filing a complaint.
32. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amounts Lost by Contact Method, Year: 2021](#) (updated Feb. 22, 2022).
33. FTC Consumer Sentinel Network, [Percentage Reporting a Fraud Loss and Median Loss by Age, Year: 2020](#) (updated Feb. 22, 2022) (Age & Fraud Losses tab with 2020 (the most recent year available) checked).
34. FTC, [Protecting Older Consumers 2020-2021](#), 34-35 (Oct. 18, 2021). This report also observed that the median loss for consumers aged 60+ was significantly higher for telephone-based frauds than other contact methods in 2020: \$1,800 for phone as compared with approximately \$1,000 for text or mail, and \$500 or less for other methods. *Id.* at 36.
35. Truecaller Insights, *supra* note 25. To underscore how severely fraud is underreported, compare Truecaller's estimates of \$10.5 billion, \$19.7 billion, and \$29.8 billion for 2019, 2020, and 2021, respectively, with the FTC's reported complaint totals of \$400,000 to \$700,000 per year for all scam calls over that same time frame. *N.B.* In both instances, these estimates include some live scam calls.
36. See *In re* Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor, [Declaratory Ruling and Third Further Notice of Proposed Rulemaking](#), CG Docket No. 17-59 and WC Docket No. 17-97, FCC 19-51, at ¶ 40 (Rel. June 7, 2019); *In re* Call Authentication Trust Anchor and Implementation of TRACED Act Section 6(a)—[Knowledge of Customers by Entities with Access to Numbering Resources, Report and Order and Further Notice of Proposed Rulemaking](#), WC Docket Nos. 17-97, 20-67, FCC 20-42, at ¶ 47 (Rel. Mar. 31, 2020); Press Release, Federal Commc'ns Comm'n, [FCC Mandates That Phone Companies Implement Caller ID Authentication to Combat Spoofed Robocalls](#) (Mar. 31, 2020) ("The FCC estimates that the benefits of eliminating the wasted time and nuisance caused by illegal scam robocalls will exceed \$3 billion annually, and STIR/SHAKEN is an important part of realizing those cost savings.").



37. See Octavio Blanco, Consumer Reports, [Mad About Robocalls?](#) (Apr. 2, 2019).
38. See Tim Harper, Consumer Reports, [Why Robocalls Are Even Worse Than You Thought](#) (May 15, 2019).
39. See Benjamin Siegel, Dr. Mark Adbelmalek, & Jay Bhatt, ABC News, [Coronavirus Contact Tracers' Nemeses: People Who Don't Answer Their Phones](#) (May 15, 2020). See also Stephen Simpson, [Few Picking Up Phone When Virus Tracers Call](#), Arkansas Democrat Gazette, July 10, 2020.
40. See Samantha Hawkins, Bloomberg Law, [Frontier Communications Sues Mobi Telecom Over Robocalls](#) (Feb. 9, 2022).
41. See Brian X. Chen, [Did You Receive a Text Message From Yourself? You're Not Alone](#), The N.Y. Times, Apr. 6, 2022.
42. See *id.* See also Verizon Community Forum, [Spam message from my own phone number?](#) (Mar. 27, 2022) (last visited Apr. 7, 2022).
43. See Federal Trade Comm'n, Consumer Advice, [How To Recognize and Report Spam Text Messages](#); Better Bus. Bureau, BBB Scam Alert: [Receive a text with a surprise offer? Don't click that link!](#) (Sept. 17, 2021); Better Bus. Bureau, BBB Tip: [Spot the red flags of fake text messages](#).
44. See AARP, Scams & Fraud, [Smishing](#).
45. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amount Lost by Contact Method](#) (updated Feb. 22, 2022) (Losses & Contact Methods tab, with years 2017 through 2021 checked). The data shows that 377,840 text scams were reported in 2021, and 90,939 in 2017. This is an increase of 286,901 complaints about scam texts, or 315%.
46. Federal Commc'ns Comm'n, [CGB—Consumer Complaints Data](#) (filtered for text messages for years 2017 and 2021). The 2017 data shows 6,093 complaints, and the 2021 data shows 14,835 complaints. This is an increase of 8,742 complaints about unwanted texts, or 143%. The FTC identifies scam texts as consumer fraud reports in which the consumer indicates that the contact method was text. See FTC Consumer Sentinel Network, [Fraud Reports by Contact Method](#) (updated Feb. 22, 2022).
47. FTC Consumer Sentinel Network, [Fraud Reports by Contact Method, Reports and Amount Lost by Contact Method, Year: 2021](#) (updated Feb. 22, 2022). The total amount of losses reported in complaints with the contact method of text message was \$37MM in 2017, and \$131MM in 2021. This is an increase of \$94MM, or 254%.
48. See *In re Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991*, Report & Order, CG Docket No. 02-278, 18 FCC Rcd. 14014, at ¶ 165 (F.C.C. July 3, 2003). *Accord In re Rules & Regulations Implementing the Tel. Consumer Prot. Act of 1991*, Declaratory Ruling and Order, CG Docket No. 02-078, WC Docket No. 07-135, 30 FCC Rcd. 7961, at ¶¶ 27, 107–108, 111–115 (F.C.C. July 10, 2015), appeal resolved, *ACA Int'l v. Federal Commc'ns Comm'n*, 885 F.3d 687 (D.C. Cir. 2018) (setting aside two parts of 2015 Declaratory Ruling, but leaving this portion undisturbed).
49. 47 U.S.C. § 227(a)(1)(A).
50. 47 C.F.R. §§ 64.1200(c)(2), 64.1200(f)(15) (definition of telephone solicitation; formerly numbered as 64.1200(f)(14) until the regulation was amended by 86 Fed. Reg. 2562 (Jan. 13, 2021)). See *Barton v. Temescal Wellness, L.L.C.*, 525 F. Supp. 3d 195 (D. Mass. 2021) (text message touting sellers' extended hours and including a link to its "menu" of goods and services was a solicitation). [The Do Not Call Registry can be found here](#).
51. 592 U.S. \_\_\_, 141 S. Ct. 1163, 209 L. Ed. 2d 272 (2021).
52. NCLC and EPIC have articulated interpretations of the *Duguid* decision that cover many of the automated dialers currently in use. See National Consumer Law Center, Federal Deception Law § 6.3.4.1 (4th ed. 2022); Electronic Privacy Info. Ctr. (EPIC), Amicus Brief,

[Evans v. Ocwen Loan Servicing, LLC, No. 21-14045](#) (11th Cir. Feb. 10, 2022); EPIC, Letter Brief, [Panzarella v. Navient Solutions, Inc., No. 20-2371](#) (3d Cir. Feb. 2, 2022); Amicus Brief, [Borden v. eFinancial, LLC, No. 21-35746](#) (9th Cir. Dec. 9, 2021).

53. 47 C.F.R. § 64.1200(f)(13). There is an additional legal theory that applies the TCPA's prohibition on prerecorded voices to text messages, but as of the time of this writing no court has recognized this theory. See *Eggleston v. Reward Zone USA, L.L.C.*, 2022 WL 886094 (C.D. Cal. Jan. 28, 2022).
54. Federal Commc'ns Comm'n, [Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information](#) (Dec. 22, 2021) [hereinafter FCC 2021 Report to Congress]. See also Molly Sinclair, [Bell Pushes 25 Cents As Nationwide Pay-Phone Rate](#), *The Wash. Post.*, Dec. 14, 1981.
55. FCC 2021 Report to Congress, *supra* note 54, at 12. See also Consumer Action, [1997 Long Distance Phone Rates Pricing Survey](#) (Feb. 1, 1997); Leslie Cauley, [Telephone Charges Creep Up Long-Distance Rates Rising After Years of Steady Drops](#), *The Baltimore Sun*, Mar. 27, 1992.
56. FCC 2021 Report to Congress, *supra* note 54, at 12 n.61 (citing to Affidavit of Joshua M. Bercu, Vice President of Policy and Advocacy for USTelecom—The Broadband Association, at 1 (Dec. 2, 2020)).
57. See Numbering Resources Report and Order, *supra* note 36, at ¶¶ 37. See also Farhan Chughtai, USTelecom, [Whitepaper: How to Identify and Mitigate Illegal Robocalls](#) 5 (Oct. 2019) at 5 [hereinafter *Identify and Mitigate Illegal Robocalls*].
58. See, e.g., Federal Commc'ns Comm'n, FCC Fact Sheet, [Targeting Gateway Providers to Combat Illegal Robocalls](#) 45 ¶ 2(d) (Sept. 9, 2021) (defining gateway providers). See also *In re Advanced Methods to Target and Eliminate Unlawful Robocalls and Call Authentication Trust Anchor*, Fifth Further Notice of Proposed Rulemaking in CG Docket No. 17-59 & Fourth Further Notice of Proposed Rulemaking in WC Docket No. 17-97, CG Docket No. 17-59 and WC Docket No. 17-97, at ¶¶ 33 (Oct. 1, 2021), (proposing definition of gateway provider) [hereinafter Oct. 1, 2021 Notice of Proposed Rulemaking].
59. See Numbering Resources Report and Order, *supra* note 36, at ¶¶ 33, 37, 47.
60. Appendix to Complaint, *United States of America v. Palumbo*, Case 1:20-cv-00473, [Declaration of Marcy Ralston at 10-12](#) ¶ 22 (E.D.N.Y. Jan. 28, 2020) [hereinafter *Declaration of Marcy Ralston*] (“With modern telecommunications infrastructure, outbound VoIP calls do not take a defined path from their origin to the final destination. Rather, the system routes calls through automated equipment that determines the lowest possible connection cost at each routing step, depending on preexisting contractual relationships between the various entities. Typically, the company at each routing step will have numerous existing contracts through which it can route outbound calls through intermediate providers to the common carriers as the last routing step before an individual in the United States can answer the call. This automated routing process is called ‘least-cost routing.’”). Marcy Ralston, a Special Agent in the Social Security Administration’s Office of Inspector General, Office of Investigations, provided a sworn statement in *United States of America v. Palumbo*.
61. See *id.*
62. See FCC 2021 Report to Congress, *supra* note 54, at 12 (“The Commission’s experience tracing back the origins of unlawful call traffic indicates that a disproportionately large number of calls originate from Voice over Internet Protocol (VoIP) providers, particularly non-interconnected VoIP providers. Moreover, the Industry Traceback Group has found that high-volume, rapid-fire calling is a cost-effective way to find susceptible targets, although it does not collect data about which robocall originators are VoIP providers.”).

63. See, e.g., Oct. 1, 2021 Notice of Proposed Rulemaking, *supra* note 58, at ¶ 33.
64. See Declaration of Marcy Ralston *supra* note 60, at 10 ¶ 20.
65. *Id.*
66. See *id.* at 12-13 ¶ 24 (“Those records further demonstrate that since at least 2016, Nicholas and Natasha Palumbo have operated TollFreeDeals as a VoIP carrier, originally out of their home in Scottsdale, Arizona, and since mid-2019 out of their current home in Paradise Valley, Arizona.”); Ryan Tracy & Sarah Krouse, [Where Robocalls Hide: the House Next Door](#), The Wall St. J., Aug. 15, 2020 (“Mr. Palumbo accumulated more than \$3.2 million on the hundreds of millions of calls routed through a telecom operation based in his Paradise Valley, Ariz., home last year.”).
67. See *In re Matters of IP-Enabled Services et al.*, Order, WC Docket No. 04-36 et al., at ¶ 6 n.19 (Rel. Oct. 9, 2007) (a VoIP service is “nomadic” if it can be used from multiple locations). A nomadic VoIP service provider can still be an interconnected VoIP provider. *In re Matters of IP-Enabled Services et al.*, Order, WC Docket No. 04-36 et al., at ¶ 3 n.8 (Rel. Apr. 4, 2008).
68. See AT&T Business, [What is VoIP and how does it work?](#).
69. See Xfinity, [What is Voice Over Internet Protocol?](#)
70. An “interconnected VoIP service” is a service that “(i) [e]nables real-time, two-way voice communications; (ii) [r]equires a broadband connection from the user’s location; (iii) [r]equires internet protocol-compatible customer premises equipment (CPE); and (iv) [p]ermits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network.” 47 C.F.R. § 9.3. See *also* 47 U.S.C. § 153(25) (incorporating this definition by reference).
71. See Declaration of Marcy Ralston, *supra* note 60, at 10 ¶ 22 (“Tracebacks of many different robocalling fraud schemes have led to the identification of Defendants as a gateway carrier willing to transmit huge volumes of fraudulent robocalls into the country, despite clear indicia of fraud in the call traffic and actual notice of fraud.”).
72. [Complaint, State of Vermont v. Bohnett](#), Case No. 5:22-cv-00069, at 9 ¶ 37 (D. Vt. Mar. 18, 2022) [hereinafter Vermont Complaint].
73. See *id.* at 9 ¶ 34.
74. According to the Industry Traceback Group, 50% of identified illegal robocalls originated in the United States. Industry Traceback Group, [Combating Illegal Calls: ITG By the Numbers](#). See *also In re Advanced Methods to Target and Eliminate Unlawful Robocalls et al.*, CG Docket No. 17-59 et al., Reply Comments of Verizon at 10 (filed Jan. 10, 2022) (observing that “bad actors would simply place more intermediate other service providers between themselves and the gateway provider, making it impossible for the gateway provider to identify and consistently stop the illegal traffic”).
75. See Vermont Complaint, *supra* note 72, at 9 ¶ 34.
76. See *id.* at 9 ¶ 35.
77. See FCC 2021 Report to Congress, *supra* note 54, at 12-13 (“Short-duration calls became popular after providers introduced six-second billing as an alternative to rounding up, as a way to become more competitive with other providers. This approach made short duration calls much less expensive, leading to a cottage industry of VoIP providers specializing in ‘dialer traffic.’ These providers compete with each other on thin margins, often with minimal staff, rented servers, online sign-ups, and virtual offices, to generate high volumes of calls. . . .”). See *also id.* at 13 n.64 (citing to Combating Robocall Fraud: Using Telecom Advances and Law Enforcement to Stop Scammers and Protect Seniors, Hearing Before the Senate Special Committee on Aging, 116th Cong. (July 17, 2019) ([written testimony of David](#)

Frankel, CEO, ZipDX LLC, at 3) (describing “small operations—a few dozen people or perhaps just one or two” that “[b]lend in robocall traffic with their other business” to supplement their bottom line)).

78. See [Great Choice Telecom](#) (ANI/ DID/CID rotator feature claims to “provide you a hands free system for Caller ID’s to change after every call made, engineered to help have more connected calls as well as stay away from scam likely”). On February 10, 2022, the FCC issued a cease and desist letter to Great Choice Telecom, requiring the provider to take mitigation steps within 48 hours and within 14 days. [Letter from FCC to Mikel Quinn, CEO of Great Choice Telecom](#) (Feb. 10, 2022). As of February 28, 2022, that language still appeared on its [website](#), and also as of May 20, 2022.
79. [Automated Number Identification](#) (ANI) is a form of caller ID. See also [Complaint for Injunctive Relief and Civil Penalties](#), North Carolina *ex rel.* Stein v. Articul8, LLC & Paul K. Talbot, Case No. 1:22-cv-00058, at 16 ¶ 60 (M.D.N.C. Jan. 25, 2022) [hereinafter Articul8 Complaint].
80. See Articul8 Complaint, *supra* note 79, at 17 ¶ 61.
81. See *id.* at 16 ¶ 60 (“For example, a legitimate telemarketer making 100,000 calls across five campaigns would typically use five different ANIs with an average of 20,000 calls per ANI. Among other things, using a single ANI for each campaign allows a legitimate telemarketer to track metrics associated with calling campaigns for different services or companies.”). See also *id.* at 18 ¶ 65 (“The average Calls-Per-ANI of [Defendant’s] calls was 1.08, which means that almost every one of the over 4.4 million calls answered came from a distinct—and likely illegally spoofed—calling number.”).
82. Declaration of Marcy Ralston, *supra* note 60, at 9 ¶ 19 (“Foreign call centers and VoIP carriers cannot connect VoIP phone traffic directly to the U.S. telephone system from a foreign location without the assistance of a U.S.-based telecommunications provider willing to accept the foreign call traffic.”). See also *United States v. Palumbo*, 448 F. Supp. 3d 257, 265 (E.D.N.Y. 2020) (“the telecommunications ‘intermediary’ industry is set up perfectly to allow fraudulent operators to rotate telephone numbers endlessly and blame other parties for the fraudulent call traffic they carry”).
83. See TRACED Act, Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019).
84. *In re Implementing Section 13(d) of the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act* (TRACED Act), Report and Order, EB Docket No. 20-22, at ¶ 1 (Aug. 25, 2021).
85. See *id.* See also <https://www.ustelecom.org/ustelecom-community/>.
86. See Vermont Complaint, *supra* note 72, at 12 ¶ 52.
87. [Industry Traceback Group, Policies and Procedures](#) 8 (revised July 2021) [hereinafter ITG Policies and Procedures].
88. See *id.*
89. See *id.*
90. Vermont Complaint, *supra* note 72, at 13 ¶ 54.
91. See Industry Traceback Group, [2021 ITG Combatting Illegal Robocalls Report 6](#) [hereinafter 2021 ITG Report]. See also ITG By the Numbers, *supra* note 74.
92. Letter from Joshua M. Bercu and Jessica Thompson, USTelecom, to Marlene Dortch, Federal Commc’ns Comm’n, [Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls](#), EB Docket No. 20-195 (filed Nov. 15, 2021) [hereinafter Bercu and Thompson Letter].
93. Articul8 Complaint, *supra* note 79, at 12 ¶ 42. See also Vermont Complaint, *supra* note 72, at 14 ¶ 57.



94. See Vermont Complaint, *supra* note 72, at 13 ¶ 53.
95. See Articul8 Complaint, *supra* note 79, at 12 ¶ 42.
96. Each traceback notice sent to every provider in the call path contains a text description of the call, typically explaining what makes it illegal. See *id.* at 30 ¶¶ 93-94 and 34 ¶¶ 98-99. In addition, most traceback notices include a link to the recorded message that was captured. North Carolina alleged that ITG notified Articul8 of this illegal traffic 49 times for calls. *Id.* at 30 ¶ 93. In one version of the Social Security scam, “the caller says your Social Security number has been linked to a crime (often, he says it happened in Texas) involving drugs or sending money out of the country illegally.” Jennifer Leach, Federal Trade Comm’n, Consumer Advice, [Fake calls about your SSN](#) (Dec. 12, 2018).
97. See Complaint for Civil Penalties, Permanent Injunction, Other Equitable Relief, and Demand for Jury Trial, *Indiana v. Startel Commc’n L.L.C.*, No. 3:21-cv-00150, 2021 WL 4803899, at ¶ 314 (S.D. Ind. Oct. 14, 2021) (“On July 22, 2020, Piratel’s CEO responded to the email, writing: ‘We will need to review internally and with USTelecom as to if we are willing to enable your trunk again. We have received 4 tracebacks in 3 weeks which is the most tracebacks we have received from any single customer, much less in the space of time.’”) [hereinafter Startel Complaint]. See also *id.* at ¶ 316 (“Despite receiving four Tracebacks, which alerted them of illegal robocalls, Piratel did not terminate Startel as a client. Quite the opposite, Startel went on to route millions more calls to Hoosiers through Piratel’s system, and Piratel continued to collect thousands of dollars from Startel.”). As a result of Indiana’s lawsuit, Piratel signed a consent decree requiring the payment of \$150,000 over five years, as well as injunctive relief including network monitoring, a prohibition on providing services to new Voice Service Provider (VSP) Customers without first engaging in reasonable screening, and the suspension of service to VSP Customers failing to meet certain requirements—without Piratel admitting fault. See Consent Decree, *Indiana v. Startel Commc’n L.L.C.*, No. 3:21-cv-00150 (Apr. 6, 2022).
98. See Articul8 Complaint, *supra* note 79, at 30 ¶ 94. In the Vermont Attorney General’s case against a gateway provider known as TCA VOIP, the defendant had been the recipient of an astonishing 132 tracebacks requests. See Vermont Complaint, *supra* note 72, at 17 ¶ 79.
99. See [Gartner Glossary, Call Detail Record \(CDR\)](#).
100. See [Re: Notice of Ex Parte Presentation by National Consumer Law Center, EPIC, Consumer Reports, National Consumers League, U.S. PIRG, and Public Knowledge to FCC Staff](#), EC Docket No. 17-97, Call Authentication Trust Anchor; CG Docket No. 17-59, Advanced Methods to Target and Eliminate Unlawful Robocalls, at 4 (filed Feb. 10, 2022).
101. Articul8 Complaint, *supra* note 79, at 18 ¶ 65.
102. See, e.g., *id.* at 3 ¶ 4.
103. See, e.g., TB Wiki, [Text Call Detail Records](#). See also CFCA KNOW Webinar, [Robocall Mitigation, What Can You Do to Prevent Illegal Robocalling?](#), at 8:00, 11:49 (Mar. 28, 2022).
104. Vermont Complaint, *supra* note 72, at 33 ¶ 123 (“Despite the Vermont Attorney General requesting TCA VOIP to place a litigation hold on CDRs during this investigation, TCA VOIP is deliberately allowing its CDRs during the investigation to be destroyed as part of a very short retention policy. As the Vermont Attorney General got better, faster access to traceback data, TCA VOIP advised its switch or software provider on January 10, 2022: ‘The AG’s have gotten faster. The latest request is for Dec 13th forward. Can you verify that the oldest is rolling off and I have 90 days of data?’”).
105. The Vermont AG based its case against TCA VOIP in part upon content analytics. See Vermont Complaint, *supra* note 72, at ¶¶ 109-11, 117 (call detail records indicating high likelihood of fraud, due to content such as “This call is from a federal agency to suspend

your social security number on an immediate basis. As we have received suspicious trails of information with your name. The moment you receive this message. You need to get back to us to avoid the consequences to connect the call immediately press one.”).

106. See, e.g., Gerry Christensen, LinkedIn, [Content-based Analytics Definitively Identifies Fraudulent Robocalls](#) (Sept. 23, 2021).
107. Electronic Privacy Information Center cautions against over-reliance on content analytics as a robocall mitigation policy, as it could lead to a regime wherein all voice messages are monitored, with or without the consumer’s knowledge.
108. *In re Call Authentication Trust Anchor, Further Notice of Proposed Rulemaking*, WC Docket No. 17-97 (Sept. 30, 2021) (Statement of Comm’r Geoffrey Starks) [hereinafter Statement of Comm’r Geoffrey Starks].
109. See CTIA, [Messaging Principles and Best Practices 15](#) (July 2019).
110. Campaign Registry, [About The Campaign Registry](#).
111. See Emily Champion, [Bandwidth Support Center, 10 DLC Overview](#) (updated Mar. 2022). Compare \$0.003 per message for registered traffic with \$0.004 per message for unregistered traffic at T-Mobile, and \$0.004 for unregistered and \$0.002 for registered at AT&T.
112. See *id.* Compare \$0.002 for political messaging with \$0.003 for insurance agents.
113. See also *Barr v. Am. Ass’n of Political Consultants, Inc.*, \_\_\_ U.S. \_\_\_, 140 S. Ct. 2335, 2344, 207 L. Ed. 2d 784 (2020) (Congress’s enactment of the TCPA “followed a torrent of vociferous complaints about intrusive robocalls. . . . Consumers were ‘outraged’ and considered robocalls an invasion of privacy. . . . In enacting the TCPA, Congress found that banning robocalls was ‘the only effective means of protecting telephone consumers from this nuisance and privacy invasion.’ ”); S. Rep. No. 102-178, at 5 (1991), reprinted in 1991 U.S.C.C.A.N. 1968, 1972–1973 (“The Committee believes that Federal legislation is necessary to protect the public from automated telephone calls. These calls can be an invasion of privacy, an impediment to interstate commerce, and a disruption to essential public safety services.”).
114. TRACED Act, Pub. L. No. 116-105, 133 Stat. 3274 (2019).
115. YouMail estimated that there were over 45.8 billion robocalls placed in 2020 and 50.5 billion calls placed in 2021. YouMail, [Historical Robocalls By Time](#). YouMail estimated that 46% of robocalls in 2020, or 21.1 billion, were scam robocalls. PR Newswire, [Americans Hit by Just Under 46 Billion Robocalls in 2020, Says YouMail Robocall Index](#) (Jan. 26, 2021). YouMail estimated that 42% of robocalls in 2021, or 21.2 billion, were scam robocalls. PR Newswire, [U.S. Phones Were Hit by More Than 50 Billion Robocalls in 2021, Says YouMail Robocall Index](#) (Jan. 6, 2022).
116. Since June 2019, the FCC has permitted (but not required) callers to block calls likely to be illegal. See Press Release, Federal Commc’ns Comm’n, [FCC Affirms Robocall Blocking by Default](#) (June 6, 2019) (“Specifically, the Commission approved a Declaratory Ruling to affirm that voice service providers may, as the default, block unwanted calls based on reasonable call analytics, as long as their customers are informed and have the opportunity to opt out of the blocking.”). Since March 2020, the FCC has stated that it expects providers’ use of call analytics supplementing STIR/SHAKEN to be sufficient to stem the tide of illegal robocalls. See Numbering Resources Report and Order, *supra* note 36, at ¶ 25 (“we expect STIR/SHAKEN paired with call analytics to serve as a tool to effectively protect American consumers from fraudulent robocall schemes”). Despite the statistical evidence of the shortcomings of these regulatory approaches, recent rulemaking proposals largely advance similar strategies. See, e.g., Oct. 1, 2021 Notice of Proposed Rulemaking, *supra* note 58, at ¶ 61 (proposing that downstream providers be required to block illegal calls only after



notification from the Commission). *But see id.* at ¶ 66 (proposing that only gateway providers be required to block calls highly likely to be illegal based on analytics), at ¶ 92 (proposing the imposition of a general duty only on gateway providers to take affirmative, effective measures rather than merely reasonable steps to combat robocalls).

117. Federal Commc'ns Comm'n, Sixth Report and Order, Seventh Further Notice of Proposed Rulemaking—CG Docket No. 17-59, [Fifth Report and Order, Order on Reconsideration, Fifth Further Notice of Proposed Rulemaking](#)—WC Docket No. 17-97 (Rel. May 20, 2022) [hereinafter Sixth Report and Order] (including a 24-hour response period for tracebacks, requiring blocking similar traffic but only upon notification from the FCC, requiring a “reasonable” Do Not Originate (DNO) List but not imposing minimum requirements and imposing limits on the scope, and holding Gateway Providers to a “reasonable steps” but not an “effective measures” standard in their robocall mitigation plans).
118. *See, e.g., In re Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, CG Docket No. 17-59, 32 FCC Rcd. 9706, at ¶¶ 9-56 (Rel. Nov. 17, 2017). The Commission also allowed providers to block all calls not on a consumer’s whitelist, which was on an opt-in basis. *Id.* at ¶¶ 26-42.
119. *In re Advanced Methods to Target and Eliminate Unlawful Robocalls, Fourth Report and Order*, CG Docket No. 17-59, FCC 20-187, at ¶¶ 39-47 (Rel. Dec. 30, 2020).
120. *See* Section III.A, *supra*.
121. *See* FCC 2021 Report to Congress, *supra* note 54, at 9; 47 C.F.R. §§ 64.6301 to 64.6304 (requiring originating providers to either implement the STIR/SHAKEN technology on their network or, if unable, to implement another robocall mitigation technology by June 30, 2021, with additional time for certain categories of voice service providers that face undue hardship; also requiring intermediate providers and terminating providers to pass along the caller ID authentication information without alteration, with two narrow exceptions); *In re Call Authentication Trust Anchor, Fourth Report and Order*, WC Docket No. 17-97, FCC 21-122 (Rel. Dec. 10, 2021) (shortening the additional time to comply for those providers likely to be the source of illegal calls); Federal Commc'ns Comm'n, Call Authentication Trust Anchor, Final Rule, 85 Fed. Reg. 73660 (Nov. 17, 2020).
122. *See* TransNexus, [Understanding STIR/SHAKEN](#).
123. A call is given a “Full Attestation (A)” when the voice service provider knows that the caller is authorized to use the calling number. “Partial Attestation (B)” means that the service provider knows the call source, but cannot verify that the caller is authorized to use the calling number. “Gateway Attestation (C)” means that the service provider knows where the call came from (i.e. either the caller, or the provider who passed the call to this provider), but cannot authenticate the call source. An example of this case would be a call received from an international gateway. *See id.* For more information on attestation, see NANC Call Authentication Trust Anchor Working Group, [Best Practices for the Implementation of Call Authentication Frameworks](#) 5, 23, and Numbering Resources Report and Order, *supra* note 36, at ¶ 8.
124. TransNexus has claimed that a greater percentage of robocalls may receive level B attestation than receive no attestation at all. *See* TransNexus, [Spam robocalls and SHAKEN attestation](#) (July 26, 2021). YouMail and Hiya have indicated that even an attestation is imperfect. *See* What Everyone Needs to Know, *supra* note 23, at slide 5 (Mar. 21, 2022); Hiya, Unexpected Effects of STIR/SHAKEN, presentation at SIPNOC 2022 Webinar Series, at slide 22 (Mar. 21, 2022).
125. *See* FCC 2021 Report to Congress, *supra* note 54, at 9; 47 C.F.R. § 64.6305(b).
126. *See* FCC 2021 Report to Congress, *supra* note 54, at 9; 47 C.F.R. §§ 64.6301 to 64.6304

- (requiring originating providers to either implement the STIR/SHAKEN technology on their network or, if unable, to implement another robocall mitigation technology by June 30, 2021).
127. *In re Call Authentication Trust Anchor, Fourth Report and Order*, WC Docket No. 17-97, FCC 21-122 (Rel. Dec. 10, 2021) (shortening the additional time to comply for those providers likely to be the source of illegal calls).
  128. See FCC 2021 Report to Congress, *supra* note 54, at 9; 47 C.F.R. § 64.6305(b).
  129. The FCC has threatened to remove non-compliant providers from the RMD on an ad hoc basis. See, e.g., [Letter from FCC Enforcement Bureau to Dominic Bohnett, CEO of Telecom Carrier Access, Inc. dba TCA Voip](#) (Feb. 10, 2022) (“downstream voice service providers will be authorized to **block all** of TCA Voip’s traffic if you do not take steps to ‘effectively mitigate illegal traffic’ within 48 hours, or if you fail to inform the Commission and the Traceback Consortium within fourteen (14) days of this letter (Thursday, February 24, 2022), of the steps you have taken to ‘implement effective measures’ to prevent customers from using your network to make illegal calls.” (emphasis in original)). However, as of the time of this writing, the Commission has never publicly announced that it removed a provider. For a list of providers who have recently received these letters, see Press Release, Federal Commc’ns Comm’n, [FCC Continues to Send Cease-And-Desist Letters to Voice Service Providers Suspected of Facilitating Illegal Robocalls](#) (Feb. 17, 2022) [hereinafter FCC Continues to Send Cease-And-Desist Letters].
  130. John Spiller, along with other individual and corporate defendants, was assessed the largest fine in FCC history in June 2020 for his role in spoofing phone numbers, calling numbers on the Do Not Call registry, and calling wireless phones without first obtaining consumer consent. See Press Release, Federal Commc’ns Comm’n, [Health Insurance Telemarketer Faces Record FCC Fine of \\$225 Million for Spoofed Robocalls](#) (Mar. 17, 2021). Biographical information about John Spiller was included on the About Us page of Great Choice Telecom, but this page has since been taken down. However, at the time of this writing, [very similar information is provided here](#). The contact information for these two organizations is identical, including the phone number and the suite number. Compare <https://web.archive.org/web/20220330212507/https://aroadtochrist.org/about-us/> with <https://web.archive.org/web/20220228151117/greatchoicetelecom.com/>. The FCC sent a cease and desist letter to Great Choice Telecom in early 2022, but did not reference [John Spiller](#). [Letter from FCC to Mikel Quinn, CEO of Great Choice Telecom](#) (Feb. 10, 2022). As this report went to print, the FCC proposed several changes to address new registrations from known bad actors. See Sixth Report and Order at ¶ 207, *supra* note 117. However, even if all of these proposals are adopted, they will not trigger automatic suspension or de-certification.
  131. See TRACED Act, Pub. L. No. 116-105, § 13(d), 133 Stat. 3274 (2019).
  132. See ITG Policies and Procedures, *supra* note 87 at 8.
  133. See FCC 2021 Report to Congress, *supra* note 54, at 16.
  134. See ITG Report, *supra* note 91, at 12; Bercu and Thompson Letter, *supra* note 92. See also ITG By the Numbers, *supra* note 74.
  135. See [Letter from FCC Enforcement Bureau to Aaron Leon, Co-Founder & CEO of thinQ Technologies, Inc.](#) (Mar. 22, 2022).
  136. See [Letter from FCC Enforcement Bureau to Vitaly Potapov, CEO, RSCOM LTD](#) (May 20, 2020).
  137. See [Letter from FCC Enforcement Bureau to Karl Douthit, CEO, Piratel, L.L.C.](#) (Feb. 4, 2020); Startel Complaint, *supra* note 97.
  138. Federal Commc’ns Comm’n, [FCC Enforcement Bureau Writes Gateway Providers on](#)

[Robocall Traceback](#) (Rel. Feb. 4, 2020); Press Release, Federal Trade Comm'n, [Globex Telecom and Associates Will Pay \\$2.1 Million, Settling FTC's First Consumer Protection Case Against a VoIP Service Provider](#) (Sept. 22, 2020).

139. See FCC 2021 Report to Congress, *supra* note 54, at Attachment A. Compare Participating tab (including all four providers listed above, as well as AT&T and Verizon) and Non-Responsive tab (containing none of the four providers listed above). See also Federal Comm'n's Comm'n, [Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information](#) (Dec. 23, 2020) (including 2019 enforcement actions in its 2020 report).
140. See FCC 2021 Report to Congress, *supra* note 54, at 16.
141. See ITG Report, *supra* note 91, at 12; Bercu and Thompson Letter, *supra* note 92. See also ITG By the Numbers, *supra* note 74.
142. See Federal Comm'n's Comm'n, [Robocall Facilitators Must Cease and Desist](#) [hereinafter Robocallers Must Cease and Desist].
143. See Articul8 Complaint, *supra* note 79, at 30 ¶¶ 94.
144. See Vermont Complaint, *supra* note 72, at 17 ¶¶ 79.
145. 47 C.F.R. § 64.1200(n)(1), *adopted by* Federal Comm'n's Comm'n, [Advanced Methods to Target and Eliminate Unlawful Robocalls, Final Rule](#), 86 Fed. Reg. 17,726, 17,727, 17,735 (Apr. 6, 2021). ("All voice service providers must . . . respond fully and in a timely manner to all traceback requests from certain entities"). Yet, no enforcement actions have been taken to date addressing a failure to comply with traceback requests. See Robocallers Must Cease and Desist, *supra* note 142.
146. Oct. 1, 2021 Notice of Proposed Rulemaking, *supra* note 58, at ¶¶ 2. The FCC also stated: "Driven in part by the rise of VoIP, the telecommunications industry has transitioned from a limited number of carriers that all trusted each other to provide accurate calling party origination information to a proliferation of different voice service providers and entities originating calls, which . . . creates new ways for bad actors to undermine trust." *Id.* The FCC cited the TRACED Act, noting that "[s]ection 6(a) of the TRACED Act also requires the Commission to 'commence a proceeding to determine how Commission policies regarding access to number resources, including number resources for toll-free and non-toll-free telephone numbers, could be modified, including by establishing registration and compliance obligations, and requirements that providers of voice service given access to number resources take sufficient steps to know the identity of the customers of such providers' within 180 after enactment." *Id.* at ¶¶ 2 n.1. See also Numbering Resources Report and Order, *supra* note 36, at ¶¶ 123-130.
147. TRACED Act, Pub. L. No. 116-105, § 6, 133 Stat. 3274 (2019).
148. 47 C.F.R. § 64.1200(n)(3), *added by* Federal Comm'n's Comm'n, [Advanced Methods to Target and Eliminate Unlawful Robocalls, Final Rule](#), 86 Fed. Reg. 17,726, 17,727, 17,735 (Apr. 6, 2021).
149. FCC 2021 Report to Congress, *supra* note 54, at 13 (citing *In re* Numbering Policies for Modern Communications et al., WC Docket No. 13-97 et al., Further Notice of Proposed Rulemaking, FCC 21-94, at ¶¶ 13 (Rel. Aug. 6, 2021) and the TRACED Act § 6(a)(1)).
150. *Id.* (citing *In re* Numbering Policies for Modern Communications et al., WC Docket No. 13-97 et al., Further Notice of Proposed Rulemaking, FCC 21-94, at ¶¶ 14 (Rel. Aug. 6, 2021)).
151. Oct. 1, 2021 Notice of Proposed Rulemaking, *supra* note 58. As this report went to print, the FCC adopted regulations requiring gateway providers to "know" their immediate upstream foreign provider. See Sixth Report and Order at ¶¶ 96, *supra* note 117. The problem with this new FCC requirement is that even for a gateway provider that "repeatedly allows a high

volume of illegal traffic onto the U.S. network,” the provider is only required to change its approach. Yet there does not appear to be sufficient incentives to ensure that the gateway will employ effective methodologies.

152. *id.* at ¶¶ 60-61. The Commission also proposed requiring providers to respond to tracebacks within 24 hours, mandatory call blocking (after receiving notice from the Commission), Know Your Customer provisions, and contractual provisions regarding mitigation (¶ 40), as well as a general mitigation standard that demands “reasonable steps” rather than effective measures (¶ 91), and certification in the RMD (¶ 94) (describing their robocall mitigation practices and stating that they are adhering to those practices). (See “Establishing the Robocall Mitigation Database” in point #4 of this section for why this last proposal is unlikely to impact robocalls.) This appears to be unchanged in the Commission’s May 20 order. See Sixth Report and Order, *supra* note 117.
153. See What Everyone Needs to Know, *supra* note 23. This appears to be unchanged in the Commission’s May 20th Order. See Sixth Report and Order, *supra* note 117.
154. See, e.g., <https://greatchoicetelecom.com/> (Great Choice Telecom advertises rotating ANIs).
155. See Federal Comm’n’s Comm’n, Numbering Policies for Modern Communications, Proposed Rules, WC Docket Nos. 13-97, 07-243, 20-67, IB Docket No. 16-155, 86 Fed. Reg. 51,081 (Sept. 14, 2021).
156. *Id.* at ¶ 4.
157. This is similar to the proposal made by USTelecom. See Identify and Mitigate Illegal Robocalls, *supra* note 57, at 8, 9.
158. Five in its 2020 report to Congress, plus one unique addition in 2021. See Federal Comm’n’s Comm’n, [Report to Congress on Robocalls and Transmission of Misleading or Inaccurate Caller Identification Information](#) (Dec. 23, 2020) (including 2019 enforcement actions in its 2020 report); FCC 2021 Report to Congress, *supra* note 54.
159. See 2021 ITG Report, *supra* note 91. See also ITG By the Numbers, *supra* note 74.
160. See Robocallers Must Cease and Desist, *supra* note 142.
161. See *In re John C. Spiller*; Jakob A. Mears; Rising Eagle Capital Group LLC; JSquared Telecom LLC; Only Web Leads LLC; Rising Phoenix Group; Rising Phoenix Holdings; RPG Leads; and Rising Eagle Capital Group—Cayman, Notice of Apparent Liability for Forfeiture, 35 FCC Rcd. 5948 (June 10, 2020).
162. See FCC Continues to Send Cease-And-Desist Letters, *supra* note 129. See also note 130, *supra*, for information about Spiller’s apparent involvement with Great Choice Telecom.
163. 16 C.F.R. § 310, *as amended by* 68 Fed. Reg. 4580 (Jan. 29, 2003). Issued pursuant to the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101 to 6108.
164. 16 C.F.R. § 310.3(b). See, e.g., *Federal Trade Comm’n v. Educare Ctr. Servs., Inc.*, 433 F. Supp. 3d 1008, 1017 (W.D. Tex. 2020). See also *Federal Trade Comm’n v. Affiliate Strategies, Inc.*, 714 F.3d 1211 (10th Cir. 2013) (writer of grant guide provided substantial assistance to fraudulent telemarketer of grant-finding services; drafted talking points for telemarketers, dealt with customer complaints, but never followed up to determine whether anyone actually received a grant); *Federal Trade Comm’n v. Partners In Health Care Ass’n, Inc.*, 189 F. Supp. 3d 1356 (S.D. Fla. 2016) (finding company that sold medical discount card and its principal liable for telemarketers’ misrepresentations; company processed all payments, fulfilled customer orders, and opened telemarketers’ merchant accounts, and principal reviewed telemarketers’ materials and handled complaints); *United States v. DISH Network, L.L.C.*, 75 F. Supp. 3d 942 (C.D. Ill. 2014) (fact question whether defendant seller of satellite TV services knew or consciously avoided knowing about one co-defendant retailer’s TSR violations; knowledge or conscious avoidance not shown as to other



retailers), *vacated in part*, 80 F. Supp. 3d 917 (C.D. Ill. 2015), *aff'd in part, vacated in part on other grounds*, 954 F.3d 970 (7th Cir. 2020); Federal Trade Comm'n v. HES Merch. Servs. Co., 2014 WL 6863506 (M.D. Fla. Nov. 18, 2014) (finding individual liability based on owner's awareness of probable fraud and intentional avoidance of the truth), *aff'd, vacated in part on other grounds*, 652 Fed. Appx. 837 (11th Cir. 2016). See also Fed. Trade Comm'n v. Global Mktg. Grp., Inc., 594 F. Supp. 2d 1281 (M.D. Fla. 2008) (U.S.-based principal whose companies processed payments for Canadian advance-fee credit-card telemarketers, fulfilled orders, handled complaints, negotiated agreements with merchants, and provided other assistance is liable for telemarketers' fraud).

165. Federal Trade Comm'n v. Consumer Health Benefits Ass'n, 2011 WL 3652248, at \*10 (E.D.N.Y. Aug. 18, 2011).
166. See, e.g., Press Release, Federal Trade Comm'n, [FTC to VoIP Providers: Turn over Information for Robocall Investigations or Prepare to be Sued in Federal Court](#) (Feb. 14, 2022).
167. See, e.g., Press Release, Federal Trade Comm'n, [FTC Takes Action against Second VoIP Service Provider for Facilitating Illegal Telemarketing Calls](#) (Dec. 3, 2020); Press Release, Federal Trade Comm'n, [Globex Telecom and Associates Will Pay \\$2.1 Million, Settling FTC's First Consumer Protection Case Against a VoIP Service Provider](#) (Sept. 22, 2020).
168. Press Release, Federal Trade Comm'n, [FTC Warns 19 VoIP Service Providers That 'Assisting and Facilitating' Illegal Telemarketing or Robocalling Is Against the Law](#) (Jan. 30, 2020).
169. Lesley Fair, [Telemarketing Sales Rule: We asked. You answered. We heard you.](#) (Apr. 28, 2022); Federal Trade Comm'n, [16 CFR 310: Telemarketing Sales Rule; Notice of Proposed Rulemaking](#) (Apr. 28, 2022); Federal Trade Comm'n, [16 Part 310: Telemarketing Sales Rule; Advanced Notice of Proposed Rulemaking](#) (Apr. 28, 2022).
170. Licensing and bonding requirements can ensure that even smaller providers can make defrauded consumers whole. See Section V, proposal 5, *infra*.
171. See, e.g., [Anti-Robocall Principles for Voice Service Providers, Principles #3 and #4](#) (2019) (statement signed by 51 state attorneys general and twelve telecommunications providers, committing to a set of principles that explicitly include requiring providers to monitor traffic on their networks and investigate suspicious patterns, and urging that providers who suspect that illegal robocalling or spoofing is occurring through their network verify that the originating commercial customer owns or is authorized to use the caller ID number, determine whether the caller ID sent matches the customer's name, terminate the party's ability to originate, route, or terminate calls, and notify law enforcement authorities); [Identify and Mitigate Illegal Robocalls](#), *supra* note 57, at 8-9 (charging originating providers with responsibility to take action where evidence suggested illegal robocalling occurred, and similarly emphasizing that downstream providers should be considered responsible for taking action when originating provider has failed to do so; urging originating providers to impose network level constraints; suggesting discontinuance of service for ongoing violations; urging FCC to require downstream providers to be alert to indicators of illegal activities and refuse to process calls from violators); [In re Advanced Methods to Target and Eliminate Unlawful Robocalls, Comments of Comcast Corporation, CG Docket 17-59 and WC Docket No. 17-97](#), at 3 (filed Dec. 10, 2021) ("while gateway providers' current obligations to respond to traceback requests and to respond to Commission notifications of unlawful traffic are significant and beneficial, they are largely *reactive* in nature, and cannot take the place of *proactive* duties to mitigate harmful traffic directed towards the United States from abroad" (emphasis in original)).

172. 47 C.F.R. § 64.1200(k)(4).
173. 47 C.F.R. § 64.1200(k)(3).
174. 47 C.F.R. § 64.1200(n)(2).
175. 47 C.F.R. §§ 64.1200(n)(3), (4) & (5). However, these providers are still permitted to continue to transmit calls into the network, until they receive notice from the Commission to stop.
176. Statement of Comm'r Geoffrey Starks, *supra* note 108.
177. The Truth in Lending Act precludes a credit card issuer from imposing liability on a customer (business or consumer) for unauthorized use of a credit card, except in narrowly defined circumstances. 15 U.S.C. § 1643.
178. See Section III, *supra* (discussing these analytics).
179. USTelecom recommended that downstream providers should be required to notify offending Originating Providers of “terms-of-service and/or acceptable-use-policy violations,” but without financial incentives these measures are likely to be inadequate. Identify and Mitigate Illegal Robocalls, *supra* note 57, at 8.
180. Suspension should result in legally effective removal from the RMD, but not physical removal. Rather, suspension should entail a prominent notation that the provider’s status is suspended. See, e.g., *In re Advanced Methods to Target and Eliminate Unlawful Robocalls et al., Comments of ZipDX L.L.C., CG Docket No. 17-59 and WC Docket No. 17-97*, at 24 (filed Dec. 7, 2021) (“We would note that ‘delisting’ should not actually constitute complete removal from the database; rather, an entry should be retained so that it is clear to all others that the problematic provider has been explicitly designated as such. This will ensure that if (when) the problematic provider attempts to shift their traffic to a new downstream, that downstream will become aware of the situation before enabling the traffic.”). As this report went to print, the FCC proposed a number of changes to how the Robocall Mitigation Database (RMD) would operate, including removing a provider from the RMD based on affiliations with a known bad actor, and revoking a provider’s international operating authority for repeat offenses. See Sixth Report and Order at ¶ 207, *supra* note 117.
181. The ITG currently considers a compliant response to be one provided within four business days (or within eight business days if the provider is new). Industry Traceback Group, presentation at SIPNOC 2022 Webinar Series (Mar. 25, 2022); ITG Policies and Procedures, *supra* note 87. As of May 20, 2022, the FCC requires gateway providers to respond to traceback requests within 24 hours, and proposed extending that requirement to all providers. See *Sixth Report and Order* at ¶¶ 65, 71, 177, *supra* note 117.
182. For example, the FCC might grant a terminating provider a safe harbor if it requires full robocall mitigation by its upstream providers, and requires that the upstream providers also require that of their upstream providers. Alternatively, a safe harbor might be considered if the provider caught and blocked the illegal traffic within a short time after their initial transmission by the provider.
183. Providers may complain that public tracebacks will expose the private agreements between providers to competitors. But this is actually a strength of this proposal, as it will give legitimate providers another incentive to identify scam calls so that those calls do not run through their networks. In addition, even publishing a scaled-back version of every traceback—including just the information regarding the caller, the originating provider, and the gateway provider and the first intermediate provider located in the U.S.—would be immensely helpful to directing resources across entities to combat the robocall scourge.