



National
Consumer Law
Center
*Fighting Together
for Economic Justice*

epic.org

ELECTRONIC
PRIVACY
INFORMATION
CENTER

SCAM ROBOCALLS: TELECOM PROVIDERS PROFIT

<https://bit.ly/Rpt-ScamRobocalls>

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.

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 of the [full report](#).