FVRO
THE FRAUD VICTIM RIGHTS ORGANIZATION

ANALYSIS

Analysis of FCC's Release of Q1, 2024 Traceback Data

Summary

On June 21, 2024 the Federal Communications Commission (FCC) released Q1, 2024 traceback data[1]. Combined with the previously released traceback data, this information further reinforces the thrust of all previous evidence: that the best way to stop illegal robocalling is at the source with diligent enforcement actions against parties that make illegal robocalls.

All traceback data released by the FCC shows there is no single gateway responsible for allowing illegal robocalls into the United States.

This data also reveals other opportunities for potential future enforcement actions to reduce robocalling though more stringent Know Your Customer (KYC) requirements for voice service providers registering with the FCC's Robocall Mitigation Database (RMD) and more thorough investigation of suspicious RMD filings.

Background

The Industry Traceback Group (ITG) is a consortium of US phone companies that collectively share information about scam robocalls in an effort to protect American consumers from fraud. ITG members provide funding to the trade association USTelecom to administer the online portal the ITG uses to trace suspected scam calls (see FVRO: **Call Tracing Demystified**)[2].

Since July 2021, complaints about unwanted calls made to the Federal Trade Commission (FTC) have declined 57%[3]. This has largely been the result deterrence promulgated by traceback requests. Criminal groups that send robocalls have learned that calls can be traced to their location and reported to law enforcement.

All objective data indicates that every successful effort to reduce robocalls has been the result of an enforcement action or fear of an enforcement action.

[1] https://www.fcc.gov/document/fcc-releases-traceback-transparency-report-1

[2] https://fraudvictimrights.org/call-tracing-demystified/

[3] https://public.tableau.com/app/profile/federal.trade.commission/viz/DoNotCallComplaints/Maps Q2 2021 v. Q1 2024.

- In 2016, IRS impersonation calls dropped 85% the day after Indian police raided six criminal call centers in Thane, India (see FVRO: **How to Stop IRS Impersonation Calls**)[4].

- In 2017, robocalling was reduced 50% after the FCC filed civil actions against Adrian Abramovich for sending millions of "neighbor spoofed" vacation and timeshare offer calls (see FVRO: **How to Stop Scam Vacation and Timeshare Calls**)[5].

- In 2018, a series of raids by local police in and around New Delhi based on tips from the Royal Canadian Mounted Police reduced Canadian Revenue Agency (CRA) impersonation calls 77% (see FVRO: **How to Stop CRA Impersonation Calls**)[6].

- Beginning in December 2019, health and health insurance related robocalls declined 60% after the FTC obtained a Temporary Restraining Order against a Canadian VoIP provider called Globex Telecom (see FVRO: **How to Stop Health Insurance Robocalls**)[7].

- Beginning in July 2021, car warranty robocalls declined 95% after the FTC opened an investigation into several telemarketing businesses. The FCC also issued notices to telecom carriers in July 2022 to disconnect a different group of businesses that had been sending car warranty robocalls (see FVRO: **How to Stop Car Warranty Robocalls**)[8].

During this same time, however, financial loss reported to the FTC resulting from fraud initiated by phone call increased 24% (see FVRO: **Robocalling Trends**)[9]. This has been the result of criminal groups in India avoiding detection though traceback by shifting from making large volumes of spoofed, outbound calls to distributing call back phone numbers through computer popup messages and e-mail.

Analysis of Q4, 2023 Traceback Data

The Q1 2024 ITG data contains 1,072 trace records from 866 suspected scam robocalls. These calls were carried by more than 235 voice service providers. Q4 data includes more than one voice service provider for many suspected scam robocalls. The FCC released data in this format data so that both the suspected "Point of Entry" into the US and the suspected originators of calls were included.

It is important to note that the designation of "Point of Entry" (POE), "Originator" (ORG) or "International Originator" (IOR) are subjective determinations manually entered by ITG staff based on their best judgement.

[4] https://fraudvictimrights.org/How-to-Stop-IRS-Impersonation-Calls/

[5] https://fraudvictimrights.org/How-to-Stop-Scam-Vacation-and-Timeshare-Calls/

[6] https://fraudvictimrights.org/How-to-Stop-CRA-Impersonation-Calls/

[7] https://fraudvictimrights.org/How-to-Stop-Health-Insurance-Robocalls/

[8] https://fraudvictimrights.org/How-to-Stop-Car-Warranty-Robocalls/

[9] https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts > Payment & Contact Methods; https://fraudvictimrights.org/Robocalling-Trends/

Without the cooperation of every phone company that transited a particular call, it may not always be clear where a call originated.

For example, the Q1 data shows Verizon as one of the top "Originators" with 18 suspected scam calls traced. While it is possible scam calls could have been sent from Verizon cell phone or VoIP numbers, it is far more likely that Verizon either could not locate the sources of these calls or the USTelecom staff chose not to list the upstream entity that sent these calls to Verizon.

In addition, sometimes attempts are made to identify the sources of calls past the US "Point of Entry." Sometimes these attempts are not made. Sometimes ITG staff send trace requests for multiple calls associated with the same the apparent scam source on the same day. This is because call records cannot always be found for specific calls. In other cases, calls from the same source may come from different voice service providers. It is therefore good practice to trace multiple calls (usually five or ten) during the same trace attempt. Sometimes, however, only single calls from a single suspected source are traced.

In order to show a more accurate and representative picture of sources of scam calls, the below tables represent "Trace Attempts" where duplicate trace requests for the same source (or "Campaign Name") through the same provider on the same day have been removed.

Call Trace Attempts by Suspected Originating Provider

The Q1 data shows no single voice service provider accounted for a majority of robocalls. The top Originator, International Originator, or Non-Responsive source accounted for 3.44% of traces. The top 10 Originators or International Originators accounted for 24.51% of traces.

Voice Service Provider	ITG Traces (De-Duplicated)	% of Traces	Top Source ("Campaign Name")
Vonage	16	3.44%	Financial-Impers-3
Verizon	16	3.44%	Authorized-Order-P2
Twilio	14	3.01%	Financial-Impers-3
Veriwave Telco, LLC	14	3.01%	HealthIns-Plan-P3
Xpertelecom Corporations	12	2.58%	ISP/Cable/Wireless-Impers-P3
Sipphony, LLC	9	1.94%	Loan-Preapproved-P1
Alliant Financial	9	1.94%	Debt-Financing-P4
DigiConnect LLC	8	1.72%	BizListing-Google-P5
Innovation Tel	8	1.72%	ISP/Cable/Wireless-Impers
Phoenix Vitae Holdings, LLC	8	1.72%	PCH-Various-P1
191 Other Providers	**351**	**75.48%**	

Of the top ten Originators:

- Two are very large, well-established US carriers.
- One is a well-established retail VoIP service provider.
- Four are small VoIP providers.
- One appears to be a debt reduction service that registered as a voice service provider.

- One appears to be a foreign provider that incorporated in the U.S. The CEO of this provider made social media posts suggesting involvement in fraud.
- One is one of six voice service providers that appear to have been registered by the same person using apparently fictitious information. These six providers may be responsible for most of the increase in robocalling complaints between Q4 2023 and Q1 2024.

It should be noted that FVRO previously forwarded confidential reports to the FCC's Enforcement Division about six voice service providers that may have registered using fictitious information. FVRO forwarded reports about two other providers that registered using stolen identities. FVRO filed a report about the above described provider that made social media posts suggesting involvement in fraud.

Implications for Policy Makers

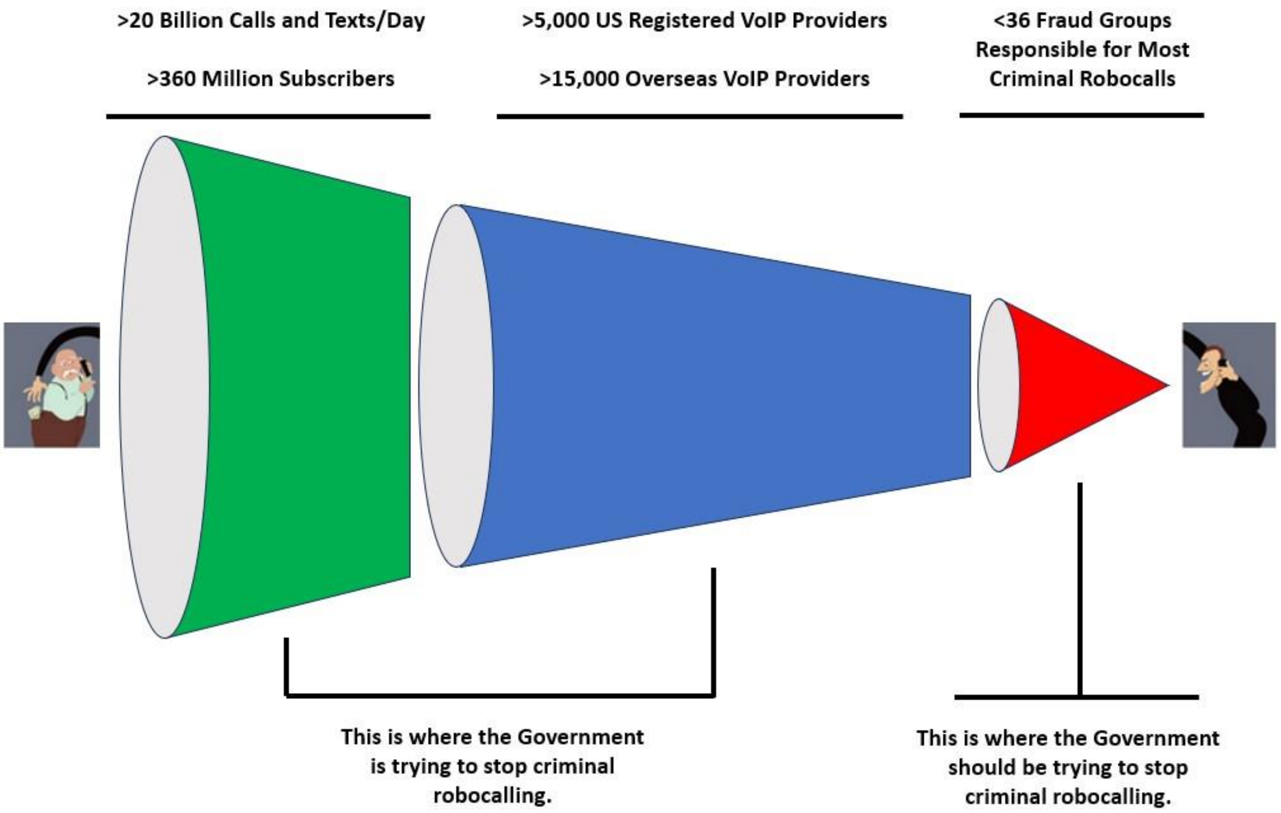
Three important facts can be derived from this ITG data.

First, all available data overwhelmingly shows that there is no such thing as a "gateway provider"—at least not in the sense that a limited number of voice service providers are "allowing" any significant portions of illegal robocalls onto US networks. There are more than 8,000 voice service providers registered in the RMD. Criminals seeking to send illegal robocalls to Americans can easily spread calls out across providers in order to avoid proactive detection. Trying to police robocalling through intermediary transit points is, at best, highly inefficient and ineffective. Illegal robocalls are most easily stopped at the source.

In the event any particular voice service provider is responsible for more than a small percentage of ITG traced calls, regulators should follow up with specific questions about measures taken to mitigate illegal calls.

- How long has the upstream provider been a customer of the "Point of Entry?"
- How long has the upstream provider been in business?
- What KYC measures were used when onboarding the upstream provider?
- Is the upstream provider still a customer of the "Point of Entry?"
- What is the upstream provider's volume of traffic?
- Where is the upstream provider located and what is their contact information?
- Did the "Point of Entry" examine the upstream provider's traffic and determine whether or not patterns matched traced calls?
- Did the upstream provider respond to traceback requests?

Otherwise, the most effective means of stopping illegal robocalls is to trace them to their source and pursue enforcement actions at the source.


>20 Billion Calls and Texts/Day
>360 Million Subscribers
>5,000 US Registered VoIP Providers
>15,000 Overseas VoIP Providers
<36 Fraud Groups Responsible for Most Criminal Robocalls
This is where the Government is trying to stop criminal robocalling.
This is where the Government should be trying to stop criminal robocalling.

Second, to this end, the FCC should comply with Section 11 of the TRACED Act (47 USC 227b–2(a)). This law requires the FCC to report evidence of criminal robocalling to the Department of Justice. Since 2020, the FCC has only made seven such referrals, even though ITG traceback data available to the FCC documents hundreds of criminal robocalling violations. Most criminal robocalls originate from overseas. The Department of Justice has the resources necessary to interface and work with foreign law enforcement agencies.

Third, the FCC’s KYC requirements for RMD registration need improvement. Such improvements will materially reduce illegal robocalls.