November 21, 2022

Marlene Dortch, Secretary
Federal Communications Commission
45 L St. NE
Washington, D.C. 20554

> **Re:** ***Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls**, EB Docket No. 20-195*

Dear Ms. Dortch:

The Industry Traceback Group (ITG)[1] is pleased to submit information for the Federal Communications Commission's annual report to Congress on the state of private-led efforts to trace back the origin of suspected unlawful robocalls.[2] In its third year as the registered consortium for private-led traceback efforts,[3] the ITG effort continues to grow as does its impact.

In 2022 to date, the ITG initiated more than 2,600 tracebacks at an average of 270 per month. The traceback initiation rate represents a 10% increase compared to last year, and nearly a 20% increase from 2020. Thanks to this accelerating rate, the ITG surpassed a milestone of 10,000 tracebacks this year, after just reaching 5,000 tracebacks in mid-2021. Because tracebacks rely on a sample of the high-volume robocall and other illegal calling campaigns on which the ITG has data, the thousands of tracebacks run by the ITG represent billions of illegal calls targeting consumers.

The ITG also continues to expand the illegal robocall campaigns it traces as well as the data sources from which it receives call examples. As shown in the figure below, two-thirds of the robocalls traced back by the ITG concern fraudulent impersonations of government agencies, utilities, and companies' brands. About one-quarter concern fraudulent and deceptive lead generation efforts where callers ignore various telemarketing requirements to deliver robocalls to hundreds of thousands of subscribers each and every day.[4] This year, the ITG also has begun to trace back illegal robocall campaigns that target Mandarin and Spanish speakers.
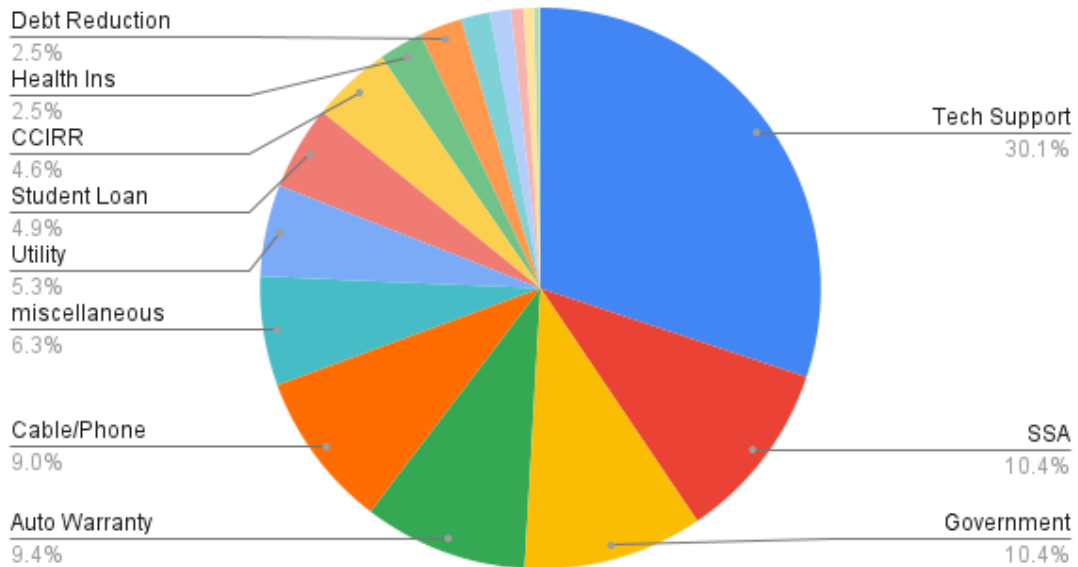
---

[1] The ITG, a collaborative effort of companies across the wireline, wireless, VoIP and cable industries actively working to trace and identify the source of illegal robocalls, is led by USTelecom. USTelecom is the premier trade association representing service providers and suppliers for the communications industry.

[2] *See* Public Notice, *Enforcement Bureau Requests Information on the Status of Private-Led Traceback Efforts of Suspected Unlawful Robocalls*, EB Docket No. 20-195, DA 22-1201 (EB rel. Nov. 16, 2022).

[3] *See 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, DA 22-870 (EB rel. Aug. 22, 2022).

[4] *See, e.g.,* FCC, Watch Out for Auto Warranty Scams, https://www.fcc.gov/consumers/guides/beware-auto-warranty-scams; FCC, Public Notice, FCC Orders Blocking of Auto Warranty Robocall Scam Campaign, July 21, 2022, https://docs.fcc.gov/public/attachments/DOC-385536A1.pdf; FCC, Consumer Alert: Be Wary of Student Loan Debt Scam Robocalls, https://docs.fcc.gov/public/attachments/DOC-388833A1.pdf; FCC Enforcement Advisory, Providers Must Aggressively Police Unlawful Robocalls Regarding Student Loans, DA 22-1145, Enforcement Advisory No. 2022-04 (rel. Nov. 3, 2022).

Active Campaigns 2022

- Debt Reduction 2.5%
- Health Ins 2.5%
- CCIRR 4.6%
- Student Loan 4.9%
- Utility 5.3%
- miscellaneous 6.3%
- Cable/Phone 9.0%
- Auto Warranty 9.4%
- Tech Support 30.1%
- SSA 10.4%
- Government 10.4%

The combination of private-led tracebacks and effective enforcement have proven to be impactful in curtailing illegal robocall campaigns. For instance, the ITG has long prioritized tracebacks of Social Security Administration impersonation robocalls, which have dropped precipitously since last year.
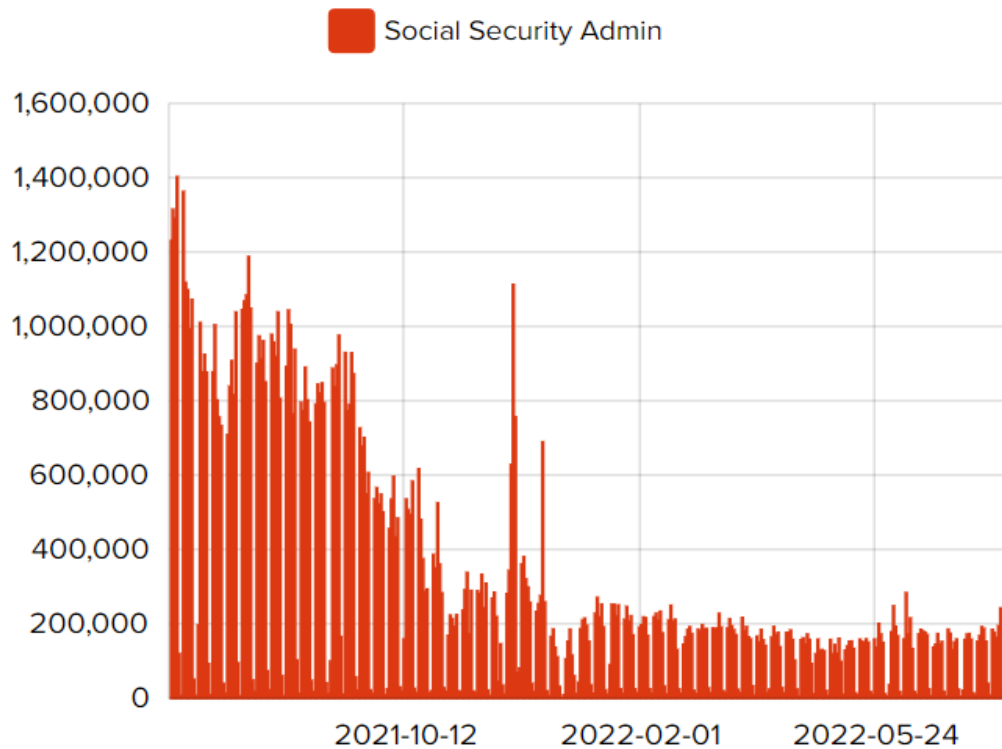
Source: YouMail

Similarly, the combination of tracebacks and enforcement by the Commission and the Ohio Attorney General led to a substantial decrease in the previously unrelenting auto warranty robocalls.
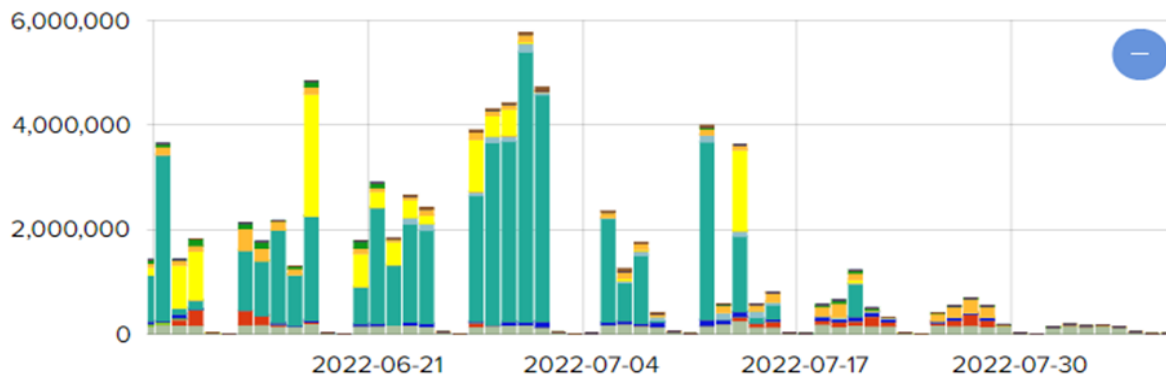

Source: YouMail

In collaboration with law enforcement and other partners, the ITG has increased the number of tracebacks of targeted, illegal and illegally spoofed calls, including threatening and/or harassing calls against individuals and organizations, fake ransom calls, and telephone denial-of-service attacks. In addition, in response to the significant increase in targeted vishing (i.e., voice phishing) attacks,[5] the ITG has increased tracebacks of such calls as well. So far this year, the ITG has completed nearly 400 tracebacks identifying the bad actors responsible for these types of attacks.

Nearly 500 domestic and foreign-based voice service providers have cooperated with tracebacks this year. Of those 500 providers, 180 were providers that had not been previously identified in ITG tracebacks, which is similar to the number of new participating providers in 2021. There were almost 50 new non-responsive providers, approximately two-thirds of which were foreign-based. The average number of providers identified in the call path of tracebacks has increased each year since 2019. This year, the ITG identified an average of 6.1 providers per traceback, up from 4.6 in 2019.

In an effort to reduce the number of persistent non-responsive providers, the ITG has implemented automated notifications to providers immediately downstream of a non-responsive provider – both before the traceback is set to time out as non-responsive and after it does so. In addition, in October 2022, the ITG launched a new feature in the ITG's Secure Traceback Portal (ITG Portal) where all participating providers can view those providers that continue to fail to respond to tracebacks. Since implementing these features, the ITG has observed an overall downward trend of tracebacks that conclude with non-responsive providers relative to the number that conclude with information about the originating provider and caller.

---

[5] *See, e.g.,* PhishLabs, *Quarterly Threat Trends & Intelligence Report*, at 13 (Feb. 2022), https://info.phishlabs.com/hubfs/PhishLabs%20-%20QTTI%20Report%20-%20February%202022.pdf.

Traceback Results Month over Month
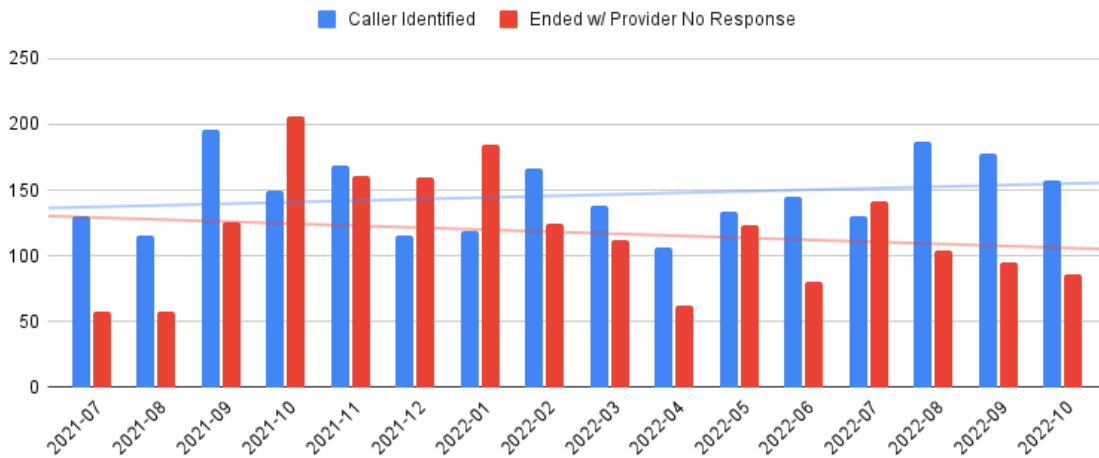
As of November 2022, ITG tracebacks have identified 146 providers as U.S.-based originating providers,[6] 82 providers as foreign-based originating providers, and 145 providers as the U.S. Point of Entry. Completed tracebacks most frequently identify callers reportedly from the United States, followed by India, Mexico, Canada, and Pakistan.

Callers Country of Origin

---
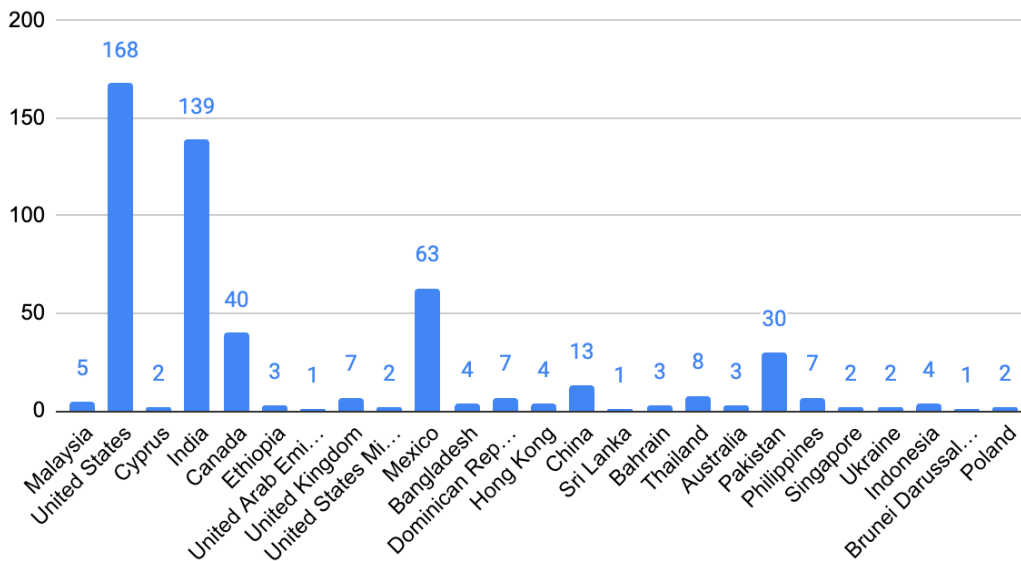
[6] The ITG generally relies on the Commission's Robocall Mitigation Database (RMD) to identify which providers are U.S.-based and which are foreign. In some circumstances a provider that claims to be U.S.-based may not in fact have any facilities, principals, or operations in the United States.

The ITG now asks that originating providers include details on the action taken with regard to the calling party. In over 70% of tracebacks, the originating provider indicates that it has terminated or warned the calling party.

Action Taken by Origin Provider

Warned calling party
21.3%

Asked calling party f...
20.0%

No Action Taken
7.8%

Terminated calling p...
50.9%
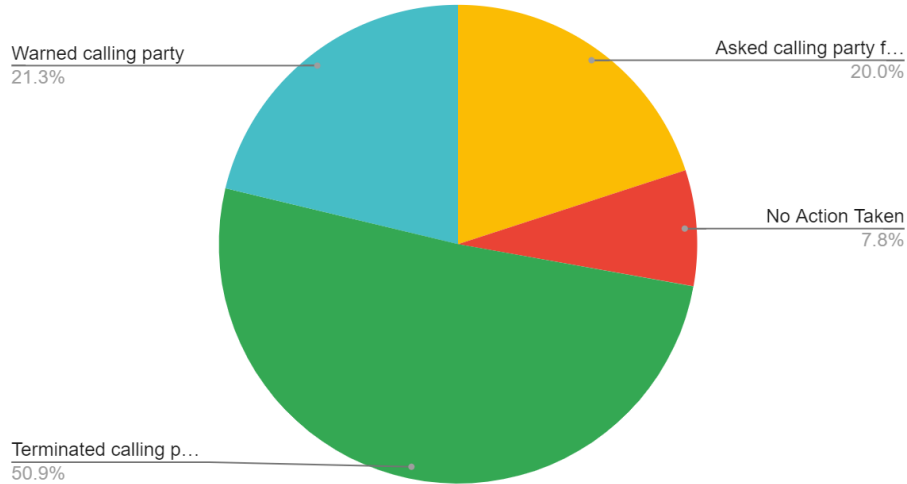
The ITG also began to fully incorporate data from the FCC's Robocall Mitigation Database (RMD) this year. As demonstrated in the chart below, about half of the providers identified in ITG tracebacks are listed in the RMD, and about half are not. Over 70% of U.S.-based providers identified in tracebacks were listed in the RMD.[7]

Provider RMD listing

Non-US no RMD
37.0%

US RMD
32.1%

US no RMD
12.3%

Non-US RMD
18.6%
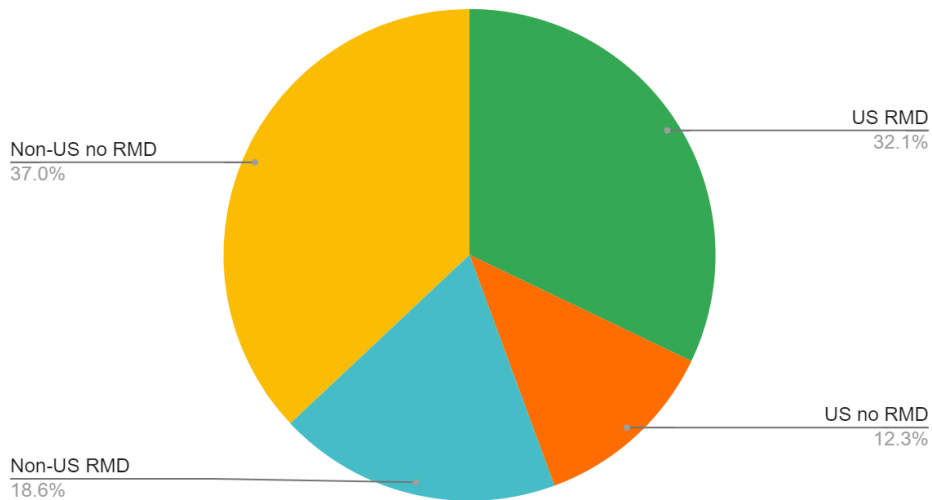
The ITG continues to build on the valuable partnership with the Commission, other federal agencies, and state law enforcement officials. The number of subpoenas and civil investigative demands to which the

---

[7] Note that many providers identified in ITG tracebacks are identified only as transit/intermediate providers, and never as originating providers.

ITG has responded continues to grow. The ITG has responded to 125 subpoenas and civil investigative demands so far this year, up from 98 last year and 75 two years ago. In addition, to supplement the information already provided to federal and state law enforcement officials, the ITG launched a new interface for direct law enforcement access to the ITG Portal in July 2022. Through the ITG Portal, law enforcement personnel can now access real-time information about which providers appear in tracebacks and how often, among other information.

Private-led traceback efforts work best and are most efficient when tracebacks and other industry actions obviate the need for law enforcement intervention. In light of this goal, the ITG launched several new features this year aimed at giving providers actionable information, including about the role their upstream providers played in the calls sent to their network. Through the ITG Portal as well as a monthly summary email, each provider today can see whether their upstream provider was subsequently identified as the originator or Point of Entry for any given traceback. This information is also available in real time to law enforcement personnel through the ITG Portal.

As noted above, law enforcement personnel now have real-time access to ITG traceback results and providers have access to actionable information they can use in their own robocall mitigation efforts. Such deliberate and intentional data sharing supports anti-robocalling efforts without unintended consequences, in contrast to the public release of raw traceback data, which can be both misleading and harmful. As the ITG has explained previously, raw traceback data may not be a meaningful indicator of a given provider's compliance with applicable law for several reasons, including differences among campaigns traced by the ITG and the call paths uncovered;[8] the gamesmanship of true bad actors seeking to evade detection;[9] and the dynamic nature of traceback.[10] Absent proper context and appropriate investigation, raw traceback data can understate the complicity of purposefully evasive bad actors while also incorrectly conveying or overstating the responsibility of other providers.[11]

In August 2022, the ITG began to collect STIR/SHAKEN information on each hop of each traceback. While some providers are still upgrading their systems so that the individuals responsible for traceback response are able to provide such information, the ITG received STIR/SHAKEN information in approximately half of the tracebacks it initiated. The ITG team is using the information to investigate signing issues and has begun to analyze attestation levels on a campaign by campaign basis, as per the chart below.
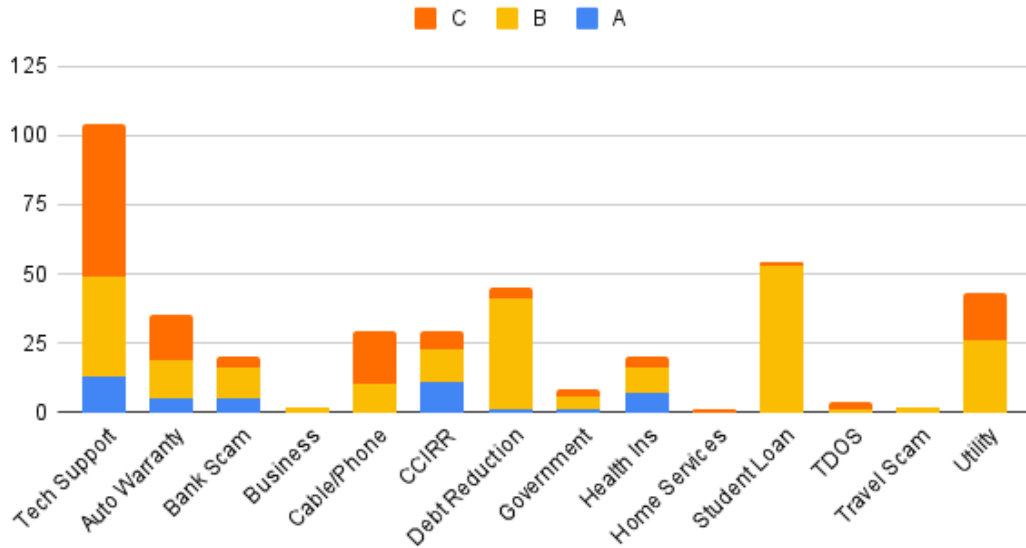
---

[8] *See* Letter from Joshua M. Bercu, Executive Director, Industry Traceback Group, to Marlene Dortch, Secretary, FCC, WC Docket No. 17-97, at 4 (filed Sept. 1, 2022).

[9] *See id.* at 5

[10] *See id.*

[11] *See id.* at 6.

Attestation by Campaign

Legend: ■ C ■ B ■ A

Campaigns (x-axis): Tech Support, Auto Warranty, Bank Scam, Business, Cable/Phone, CCIRR, Debt Reduction, Government, Health Ins, Home Services, Student Loan, TDOS, Travel Scam, Utility

y-axis scale: 0, 25, 50, 75, 100, 125

The ITG team anticipates making additional use of STIR/SHAKEN information as it is collected at full scale.

*   *   *

The ITG stands ready to continue to assist the Commission and other government and industry stakeholders in stopping the scourge of illegal robocalls and protecting users of the phone network. The ITG encourages the Commission to continue its work with federal and state law enforcement partners to bring aggressive enforcement against robocallers at home and abroad, as well as those voice service providers responsible for the illegal robocall problem.

Please contact the undersigned if you have any questions.

Sincerely,

   /s Joshua M. Bercu/

Joshua M. Bercu
Executive Director
Industry Traceback Group

Jessica Thompson
Director of Traceback Operations
Industry Traceback Group