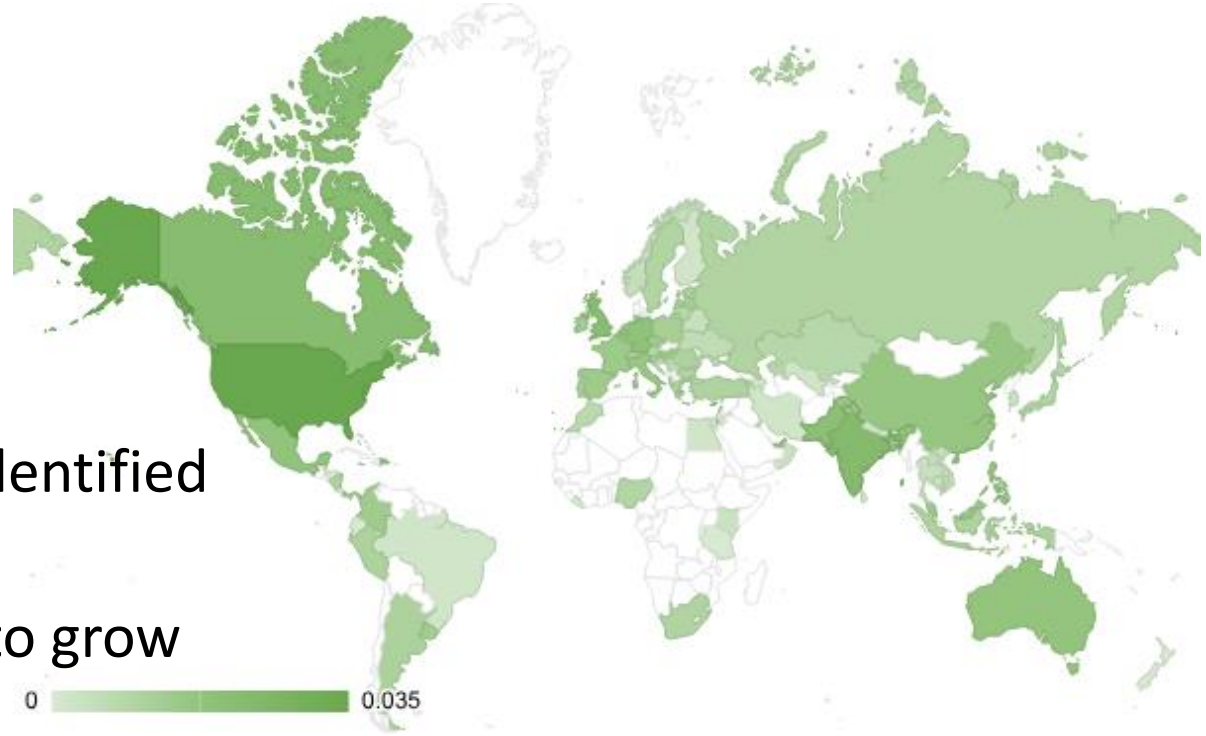
The State of Industry Traceback 2025

Agenda

1. The State of Industry Traceback
2. The Decline in Tracebacks Identifying Non-U.S. Providers
3. Provider Churn
4. Reports of Hacking/Compromised Systems
5. Case Study
6. On the Horizon

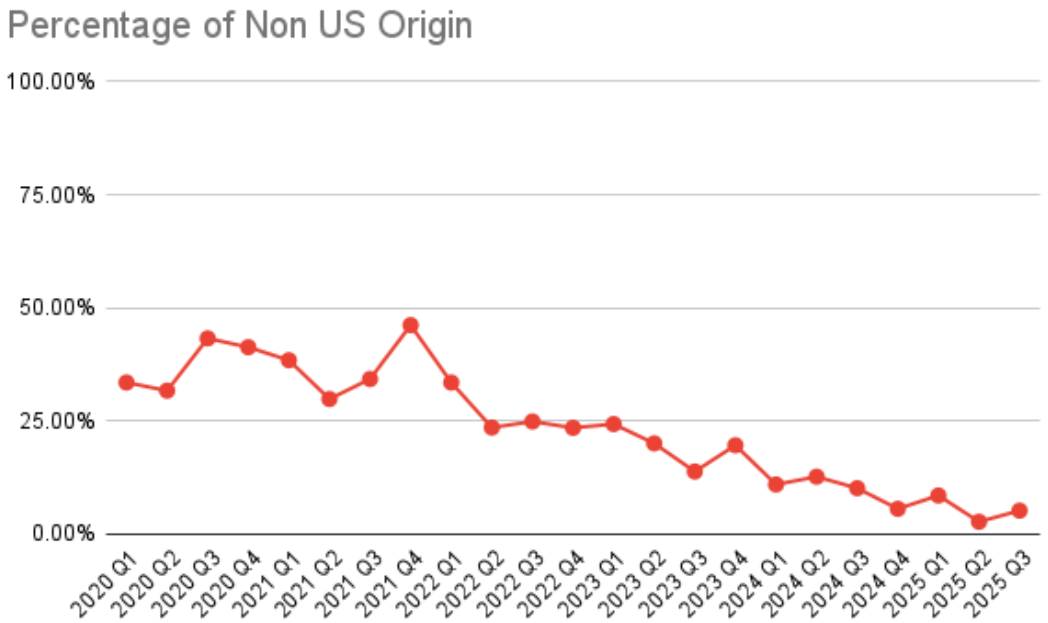
State of Industry Traceback

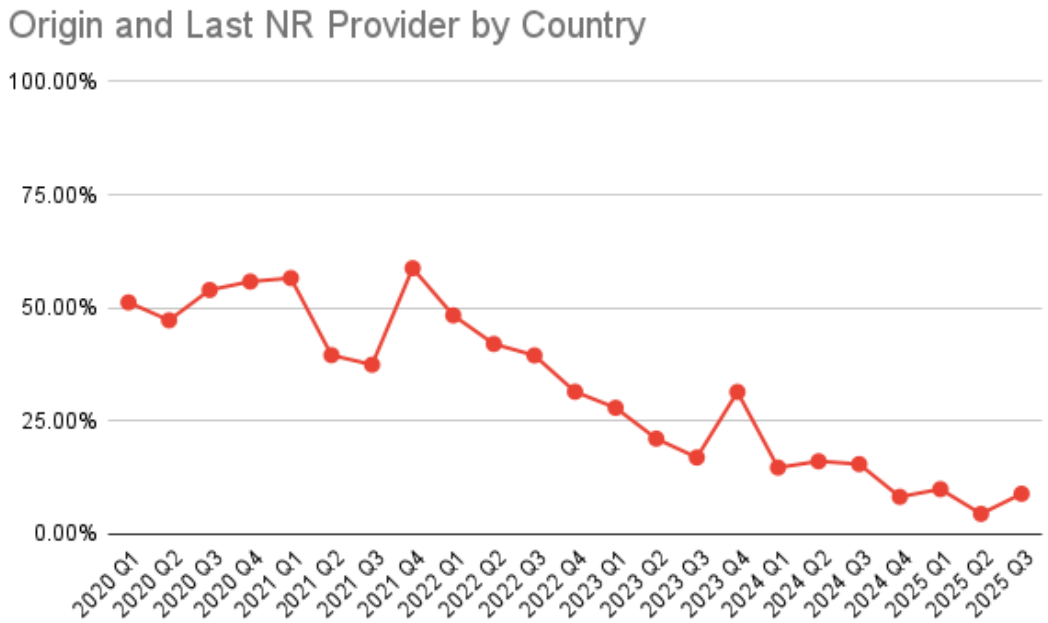
- Initiated over 32,000 tracebacks which include a full gamut of illegal calling:
  - unsolicited telemarketing robocalls
  - scam robocalls
  - targeted scams
  - swatting and active threat calls
- Over 2,300 U.S. and foreign providers identified from 90 countries
- Work with law enforcement continues to grow



INDUSTRY TRACEBACK GROUP

Observation #1 - Decline in Tracebacks Identifying Non-U.S. Providers





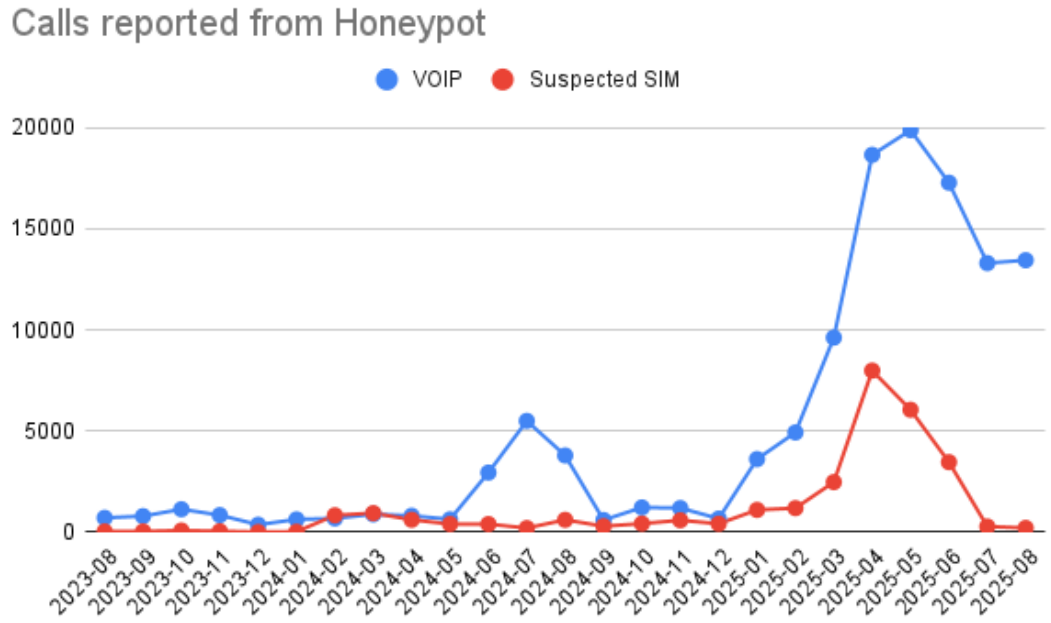
INDUSTRY TRACEBACK GROUP

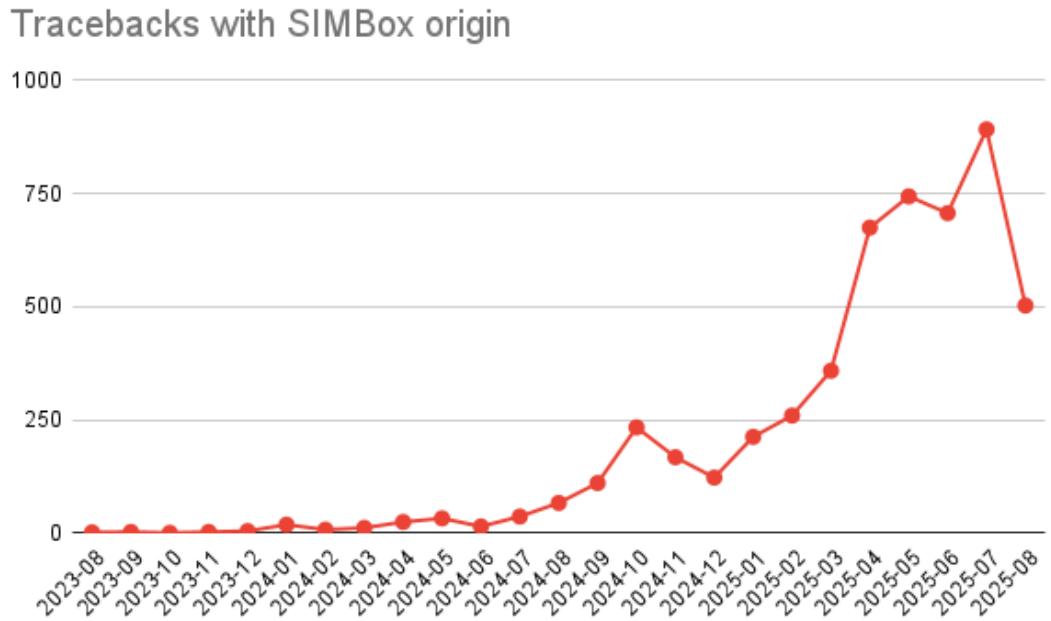
Potential Causes of the Decline

- Foreign-entities incorporating in and registering as U.S.-based
  - ITG has previously identified, for instance, disproportionate number of Wyoming-based voice service providers in tracebacks
- SIMBoxes
  - Relatively new trend for voice calling but an active area for ITG with over 5,000 number of tracebacks of SIM-based calling

SIMBox Origination

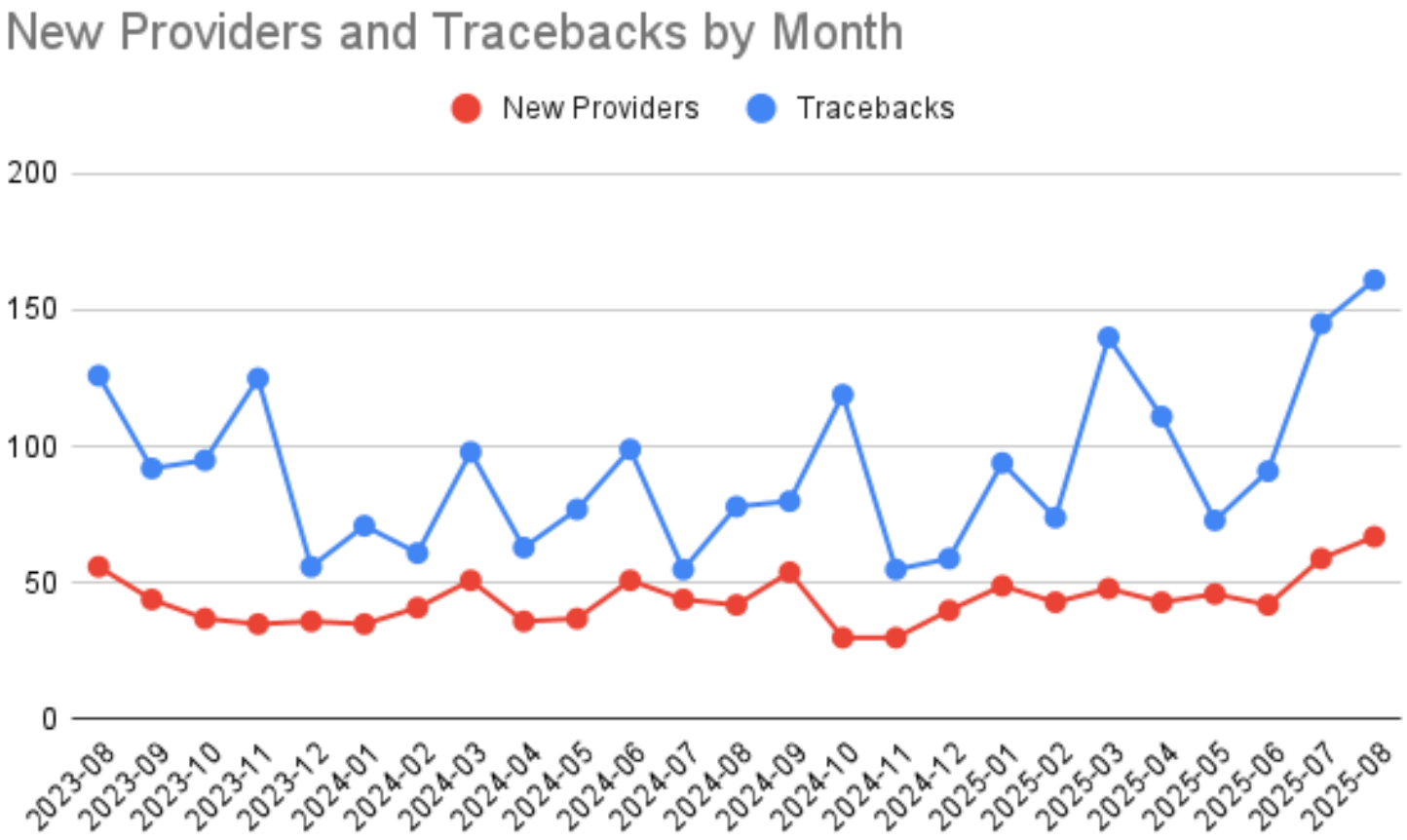
- Historically used for text, but now used for calls
- Amazon/order scam, bank/government impersonations, package delivery, sweepstakes, etc.





INDUSTRY TRACEBACK GROUP

Observation #2 - Provider Churn



INDUSTRY TRACEBACK GROUP

Possible Reasons for the Churn…

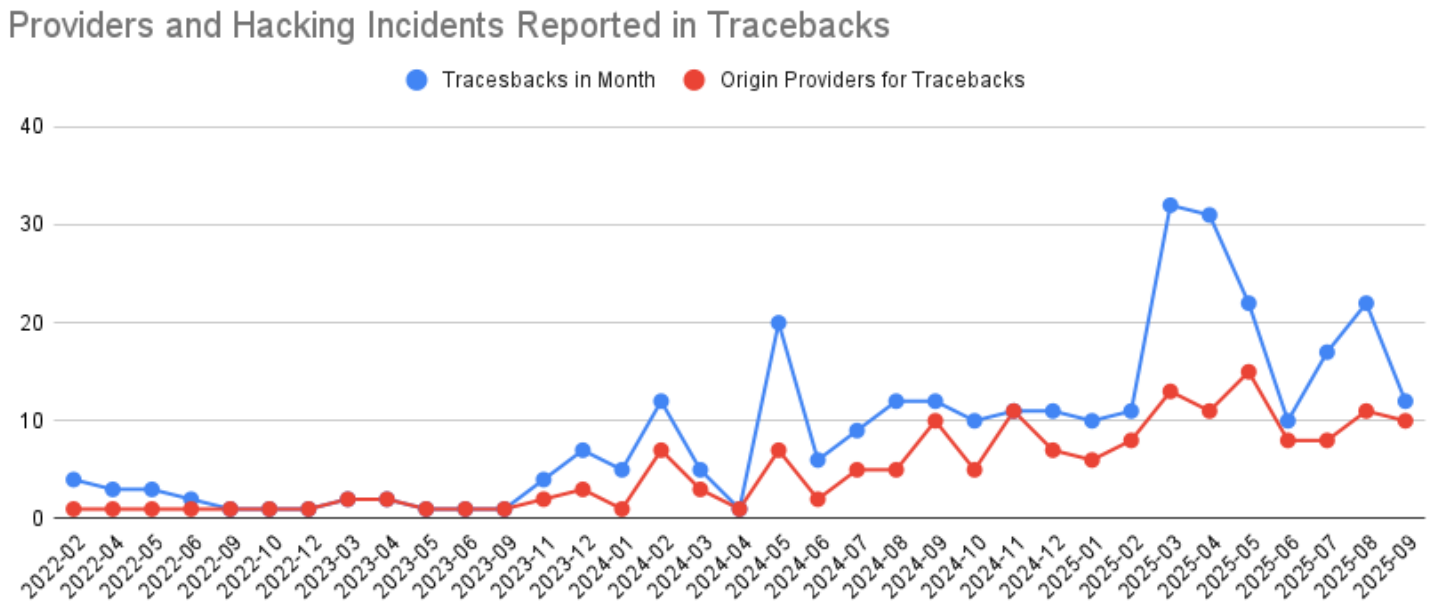
- Increased disruption pre-enforcement just due to traceback
- Some expansion of breadth of traceback work
- Proliferation of shell company providers/alter egos

Digging In: The Presumed Existence of Alter Egos

- ITG has identified voice service providers that appear to be alter egos
- 48 providers in 7 groups that always show up near each other in call path
- Many end up downstream of potentially affiliated non-responsive providers, trying to add distance and plausible deniable to downstream partners
- Irregular call signing
- ITG has made numerous referrals to law enforcement agencies

Observation #3 – Reports of Hacking/Compromised Systems

- Rise in hacked PBXs and compromised credentials starting in 2024.
- Tactic that used to be reserved for traffic pumping became employed for robocalls and targeted bank scams.
- Over 70 providers reported incidents in 175 tracebacks in past year.
- Identification of problem through traceback seems to help in patching and preventing further occurrences.



Case Study – Hacked School System

Recently, we assisted in tracing a sophisticated bank scam to the origin, a hacked school system.

Pre-recorded calls went out and included a callback number. In running tracebacks and traceforwards we found multiple systems were compromised to:

- Send the call traffic from a compromised system which signed calls with A attestation
- Call back numbers forwarded from a compromised 800 to a voip DID which was also compromised to receive.

On the Horizon

- Increasing interest in traceback abroad
- Working on ITG guidance for enterprise/PBX call system security
- Monitoring closely for providers on FCC delisting, as well as impact of that FCC action
- We are increasingly called on to address calls beyond robocalls, not just scams, but those that threaten public safety.