

TRACED Act Compliance

Everything you need to know

February 18, 2021

Speakers



Jim Dalton
TransNexus Inc.
CEO



Kevin Rupy
Telecom Partner
Wiley Rein



Alec Fenichel
TransNexus Inc.
Senior Software Architect

Agenda

- FCC Requirements
- ClearIP Robocall Mitigation Tools
- Non-IP Call Authentication Update
- Questions and Answers

wiley

The FCC's Robocall Mitigation Plan Requirements, Explained



Kevin G. Rupy
krupy@wiley.law

February 18, 2021



High Level Takeaways from FCC Robocall Activities

- Since passage of the TRACED Act in late 2019, the FCC has been ***rapidly implementing*** its anti-robocall provisions;
- Recent actions by the FCC include ***several mandates for voice providers, including robocall mitigation plans***;
- Voice providers subject to any FCC STIR/SHAKEN extension ***must implement a robocall mitigation plan by June 30, 2021***;



An Additional High Level Takeaway

The Communications Act and '96 Act Created Narrow Regulatory Categories:

- ILECs/CLECs
- Cable Providers
- Wireless Providers
- Interconnected VoIP
- Non-Interconnected VoIP
- Information Services

- The TRACED Act Wipes Away Those Distinctions:
 - Providers of “voice service.”

37. For purposes of our rules, we also adopt a definition of “voice service” that aligns with the TRACED Act. The TRACED Act employs a broad definition of “voice service” that includes “without limitation, any service that enables real-time, two-way voice communications, including any service that requires [I]nternet [P]rotocol-compatible customer premises equipment . . . and permits out-bound calling, whether or not the service is one-way or two-way voice over [I]nternet [P]rotocol.”¹⁴¹ The TRACED Act definition is limited, however, to service “that is interconnected with the public switched telephone network and that furnishes voice communications *to an end user*.”¹⁴² Thus, the rules we adopt today apply to originating and terminating voice service providers and exclude intermediate providers.

Report and Order and Further Notice of Proposed Rulemaking, WC Docket Nos. 17-97, 20-67, FCC 20-42, March 31, 2020.



Key Components of Recent FCC Activity

Second Report and Order (FCC 20-136; Oct. 1, 2020)

- Establishes caller ID authentication ***obligations*** in non-IP networks;
- Establishes frameworks for ***exemptions*** from and ***extensions*** of the June 30, 2021 STIR/SHAKEN mandate deadline;
- Requires a ***robocall mitigation program*** for any voice service provider subject to a STIR/SHAKEN deadline extension;
- Mandates ***registration and certification framework*** for all voice providers;
- Prohibits intermediate and terminating providers from accepting traffic from ***non-compliant providers***; and



Key Components of Recent FCC Activity

Fourth Report and Order (FCC 20-187; Dec. 30, 2020)

- Places *affirmative* robocall mitigation obligations on *all* voice providers to:
 - Respond to traceback requests;
 - Take steps to “effectively mitigate” illegal traffic when notified; and
 - Prevent new and renewing customers from originating robocalls.
- Expands safe harbor based on reasonably analytics to network-based blocking;
- Establishes enhanced transparency and redress requirements;



wiley

How to Approach Robocall Mitigation Plans



Extension Recipients Must Implement Mitigation Plans

Small/Rural Voice Providers

- 100,000 or fewer voice subscriber lines
- Two-year extension - June 30, 2023

Inability to Obtain STIR/SHAKEN Tokens

- Cannot obtain certificates necessary to participate in STIR/SHAKEN
- Indefinite extension
- Note recent action by STIR/SHAKEN GA

Pending 214 Applicants

- Must be subject to a pending Section 214 discontinuance application
- One year from date of filing (no later than June 30, 2021)

Networks Incompatible with SIP

- Networks reliant on technology that cannot initiate, maintain, and terminate SIP calls
- Indefinite extension (until a solution is “reasonably available”)



Mitigation Plans: FCC Guidance and Requirements

- Voice service providers subject to an extension must implement an appropriate robocall mitigation program to prevent unlawful robocalls from **originating** on their network.
- FCC generally takes a “***non-prescriptive*** approach.”
- Robocall mitigation programs will be deemed sufficient if the voice service provider:
 - (1) ***includes detailed practices*** that can ***reasonably be expected*** to significantly reduce the ***origination of illegal robocalls***,
 - (2) ***complies with*** the practices it describes, and
 - (3) ***participates in*** industry traceback efforts.
- Voice service provider must “document and publicly certify how they are complying.”
- FCC’s Enforcement Bureau to impose on a voice service provider more prescriptive measures where its robocall mitigation program is deemed insufficient.



Building Blocks to a Successful Mitigation Plan

Implement FCC Requirements

- Several FCC orders have identified certain requirements (e.g., participating in traceback).

Integrate Existing Procedures

- Must be expected to “**significantly reduce** the origination of illegal robocalls.”

Incorporate Additional Tools & Measures

- **Not** a filing exercise: plans must be implemented.
- Companies must commit to outlined measures.

Avoid Costly Obligations

- FCC can “impose **more prescriptive** obligations.”
- Providers could be subject to **FCC enforcement**.
- Removal from FCC database – traffic shut down.

Wiley Can Draft and Submit Your Mitigation Plans

- Request tailored Mitigation Plan Questionnaire (available late Feb. 2021).
- Complete and Return the Mitigation Plan Questionnaire to your Wiley attorney.
- Wiley staff will closely coordinate with you on compiling and submitting your mitigation plan to the FCC.

Wiley is Uniquely Qualified on the Robocall Issue

- Wiley attorneys have been advocating and developing policy on the robocall issue for nearly the last decade.
- Our stable of professionals include attorneys that:
 - Have represented some of the largest and most prominent companies and trade associations operating in this space;
 - Delivered expert testimony before the Senate on numerous occasions on the topic of TCPA compliance, TRACED Act implementation and robocalls;
 - Regularly present to professional organizations and the media on the robocall topic; and
 - Developed and led the USTelecom Industry Traceback Group.



ClearIP Robocall Mitigation Tools

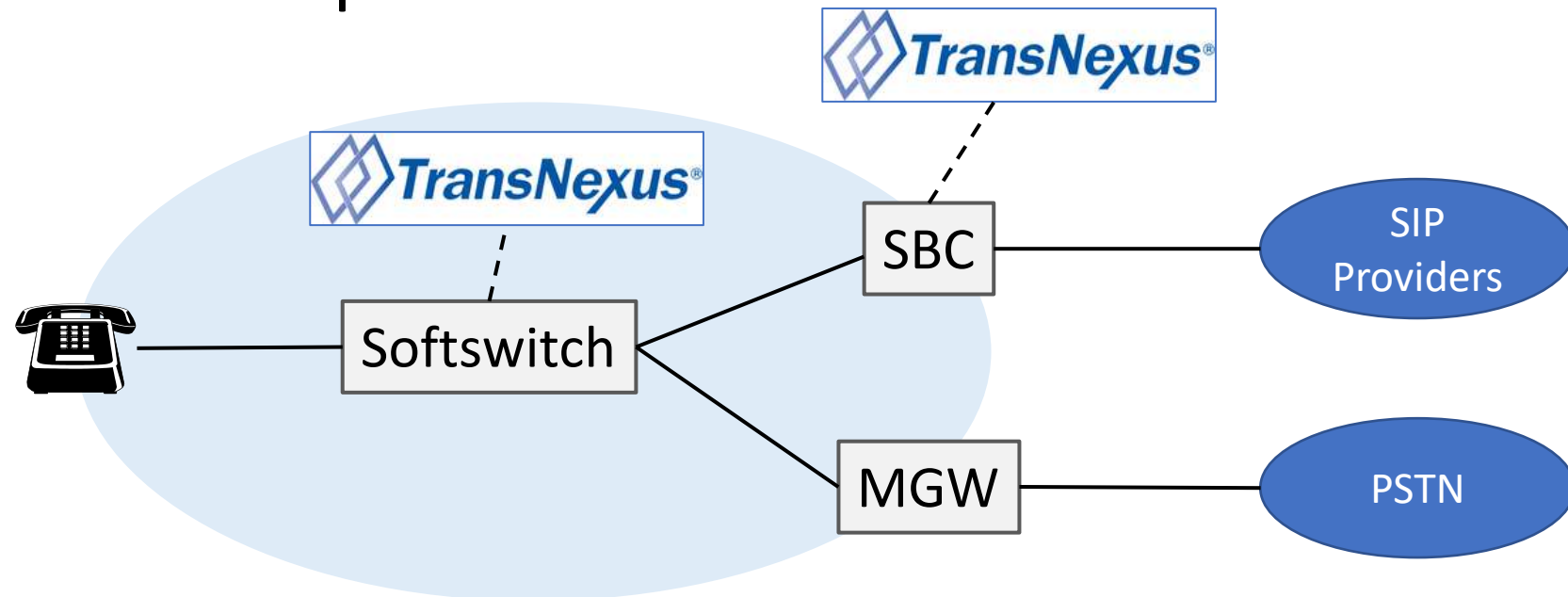
- Calling number controls
- Real time reports for problematic calling numbers:
 - Invalid
 - Do Not Originate (DNO)
 - Bad reputation (marked as spam in call analytics)

TransNexus Robocall Mitigation Benefits

- Full compliance with FCC requirements
 - Ensure only ~~valid~~ pristine calling numbers egress your network
- Identify good subscriber calling numbers that are labeled as spam
 - Restore good subscriber calling number's reputation
- Real time analytics and control
- Simple

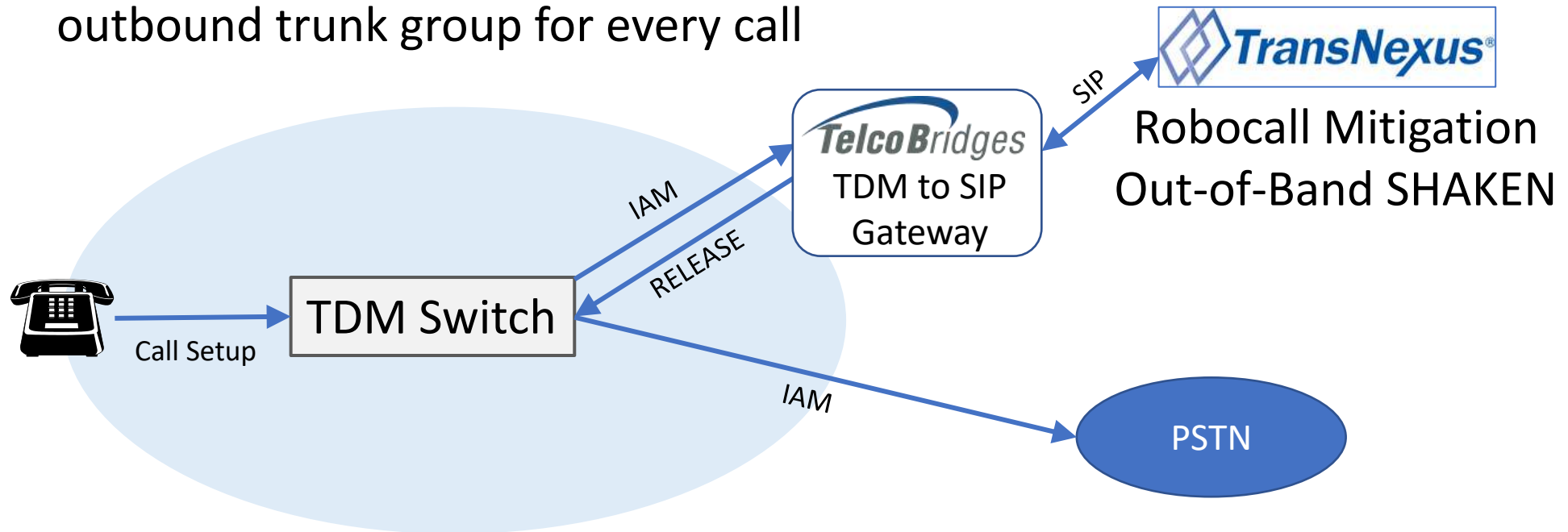
Simple, Flexible Network Integration

- Centralized deployment or at the network edge
- SIP and HTTP SHAKEN interfaces
- Cloud or on-premises



Integration for TDM switches

Configure TransNexus as the first
outbound trunk group for every call



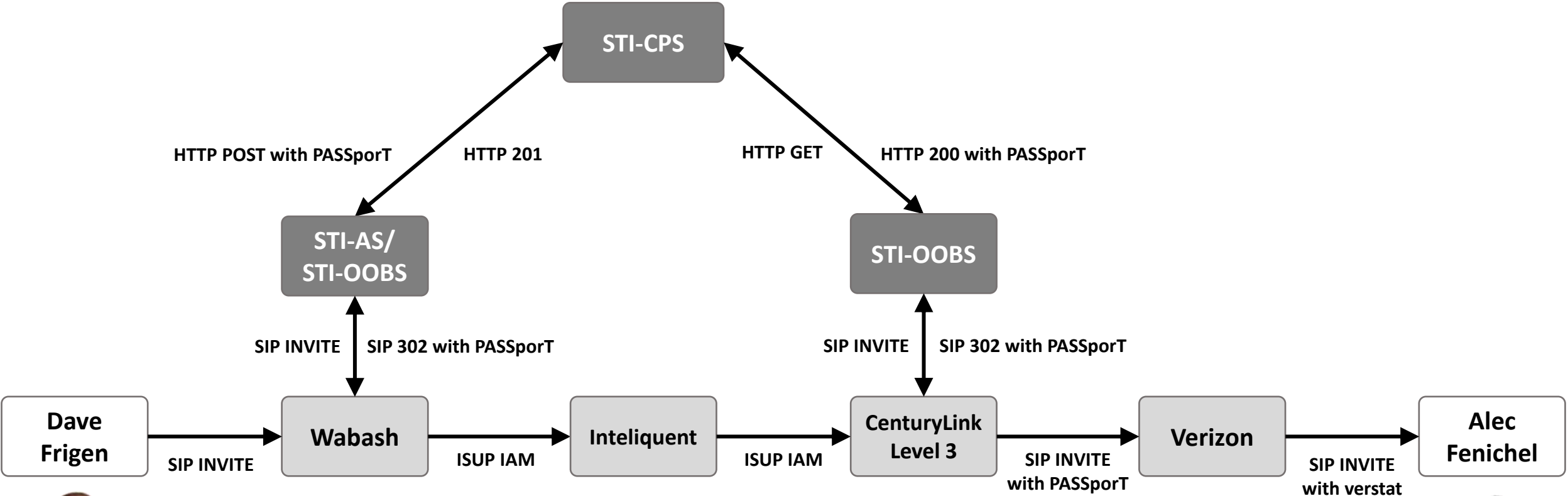
Route advance to next
trunk group to complete call

Demo of Robocall Mitigation Tools

Non-IP Call Authentication Update

- ATIS PTSC Non-IP Call Authentication Task Force created in May 2020
- *Out-of-Band Token Transmission for TDM Networks*
 - Extends SHAKEN to TDM networks
 - Co-authored by
 - NetNumber
 - NeuStar
 - TransNexus
 - Approval expected in April 2021

Non-IP Call Authentication – How it Works



Demo of SHAKEN Features

Questions & Answers

How to get started?

- Contact Kevin Rupy KRupy@wiley.law for FCC compliance questions
- Contact Jim.Dalton@TransNexus.com for a demo and technical information