TransNexus®

Compliance 101

New Robocall Mitigation Rules

Presenters

Jim Dalton

Chief Executive Officer

TransNexus

Donald St Denis

Product Marketing Manager

TransNexus

About TransNexus

- A leader in developing innovative software to manage and protect telecommunications networks since 1997
- Active participant with telecommunications industry standards work groups

- STIR/SHAKEN
- SHAKEN Certificates
- Out-of-Band Call Placement Service
- Branded Calling
- Robocall Mitigation and Prevention
- TDoS Prevention
- Toll Fraud Prevention
- Least Cost Routing
- Analytics
- Billing Support

The SIP School

Learn and Qualify

www.thesipschool.com

SIP SSCA® ELITE

The SIP School
Certified Associate

Advocates for Rural Broadband

w-t-a.org

Advocacy

Member Service

Communications

Education

Agenda

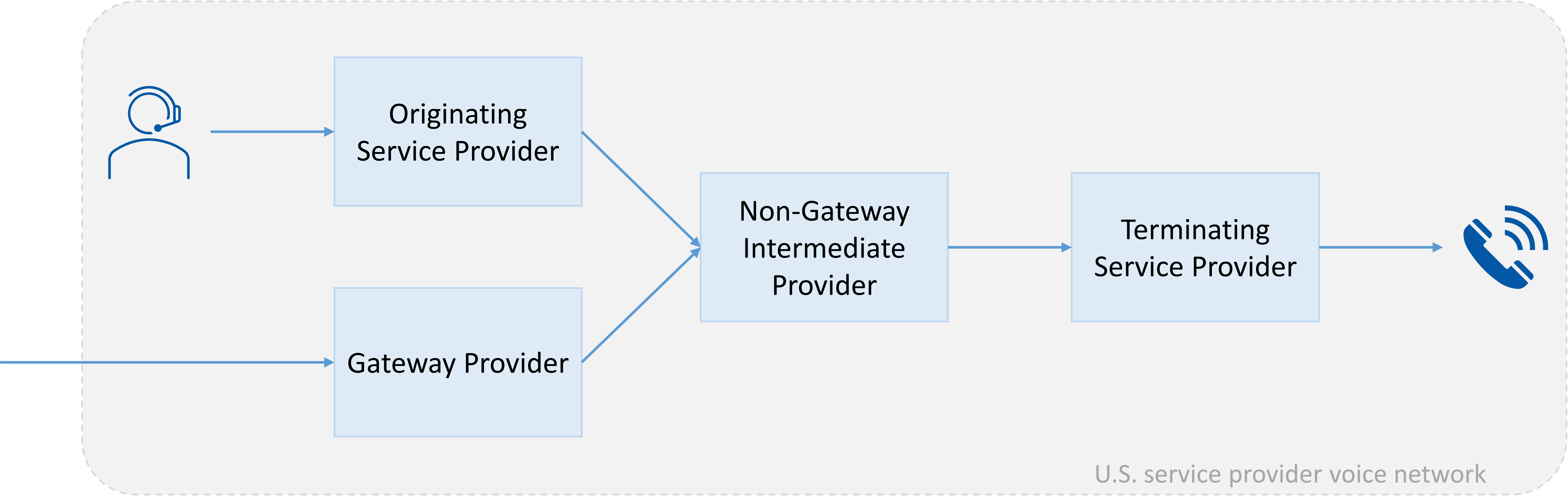
A review of new rules for robocall mitigation and call authentication

1. Robocall mitigation
2. Robocall Mitigation Database (RMD)
3. STIR/SHAKEN by non-gateway intermediate providers

- Ask questions using **Q&A** (not Chat)
- Slides on transnexus.com tomorrow
- Consult your attorney for legal advice

Robocall Mitigation

Provider roles (“call-by-call basis”)



Originating Service Provider

Gateway Provider

Non-Gateway Intermediate Provider

Terminating Service Provider

U.S. service provider voice network

Robocall blocking and mitigation timeline

2017
2018
2019
2020
2021
2022
2023
2024

November 16, 2017:	Call blocking **allowed** for calls from invalid, unallocated, unused, DNO numbers.
June 6, 2019:	Call blocking **allowed** on opt-out basis using any reasonable analytics.
June 30, 2021:	Mitigation **required** on unauthenticated calls originated.
January 16, 2023:	Mitigation **required** on inbound NANP calls transited by gateway providers.
January 8, 2024:	Mitigation **required** on all NANP calls, all providers.

Includes links to the Code of Federal Regulations and Federal register.

“Reasonable”

- “A robocall mitigation program is **sufficient** if it includes detailed practices that can reasonably be expected to significantly reduce the origination of illegal robocalls.”
- “A mitigation program **insufficient** if a provider knowingly or through negligence serves as the originator for unlawful robocall campaigns.”
- Second Order ¶ 78

“Call blocking” versus “robocall mitigation”

- “Voice service providers may block calls so that they do not reach a called party.”
  - 47 CFR 64.1200(k)
  - Must not block emergency calls

- “The term *effectively mitigate* means identifying the source of the traffic and preventing that source from continuing to originate traffic of the same or similar nature.”
  - 47 CFR 64.1200(f)(18)

Requirements by role

Provision	Originating Service Provider	Gateway Provider	Non-Gateway Intermediate	Terminating Service Provider
Block Invalid, Unused, Unallocated	Optional	Mandatory	Optional	Optional
Block Do-Not-Originate	Optional	Mandatory	Optional	Optional *
Block using reasonable analytics on opt-out basis				Optional *
Mitigate traffic when notified by the FCC	Mandatory		Mandatory	Mandatory
File a certification in the RMD‡	Mandatory	Mandatory	Mandatory	Mandatory
Accept NANP traffic only from providers with an RMD filing	Mandatory	Mandatory	Mandatory	Mandatory
Take affirmative effective measures to prevent customers originating illegal calls	Mandatory			

* FNPRM 8 proposes making these provisions mandatory.

As of July 11, 2023. Includes links to the Code of Federal Regulations.

Requirements by role

Provision	Originating Service Provider	Gateway Provider	Non-Gateway Intermediate	Terminating Service Provider
Take reasonable effective steps to ensure direct upstream providers are not sending high volume of illegal traffic		Mandatory	January 8, 2024	January 8, 2024
File a robocall mitigation plan in RMD‡	If no SHAKEN; all January 8, 2024	Mandatory	January 8, 2024	January 8, 2024
24-hour Traceback Response	January 8, 2024	Mandatory	January 8, 2024	January 8, 2024
Cease carrying illegal traffic when notified by the FCC	January 8, 2024	Mandatory		
Block traffic received directly from a provider that failed to cease carrying illegal traffic after FCC notification			If upstream is gateway; all January 8, 2024	If upstream is gateway; all January 8, 2024

‡ Also applies to providers without the facilities necessary to implement STIR/SHAKEN (Sixth Order ¶ 37).

As of July 11, 2023. Includes links to the Code of Federal Regulations and the Federal Register.

Examples of vetting provisions (not prescriptive)

- Name, physical and mailing addresses, contact telephone numbers, and email addresses of principals and controlling persons of the entity, any persons with a majority ownership interest in the customer, staff responsible for compliance with TCPA, TSR, and other such laws.
- For those involved in telemarketing: Customers' subscription account number for the DNC Registry, Universal Service Fund registration number, a copy of their FCC 499, and Section 214 International Authority (if applicable).
- Federal taxpayer ID
- Trade or bank references for high-risk customers
- Copy of customer's written policies for complying with the TCPA, TSR, traceback requests, robocall mitigation, etc.
- History of traceback requests
- Telephone numbers used for caller ID and proof of authority to use them

Examples found in legal consent agreements.

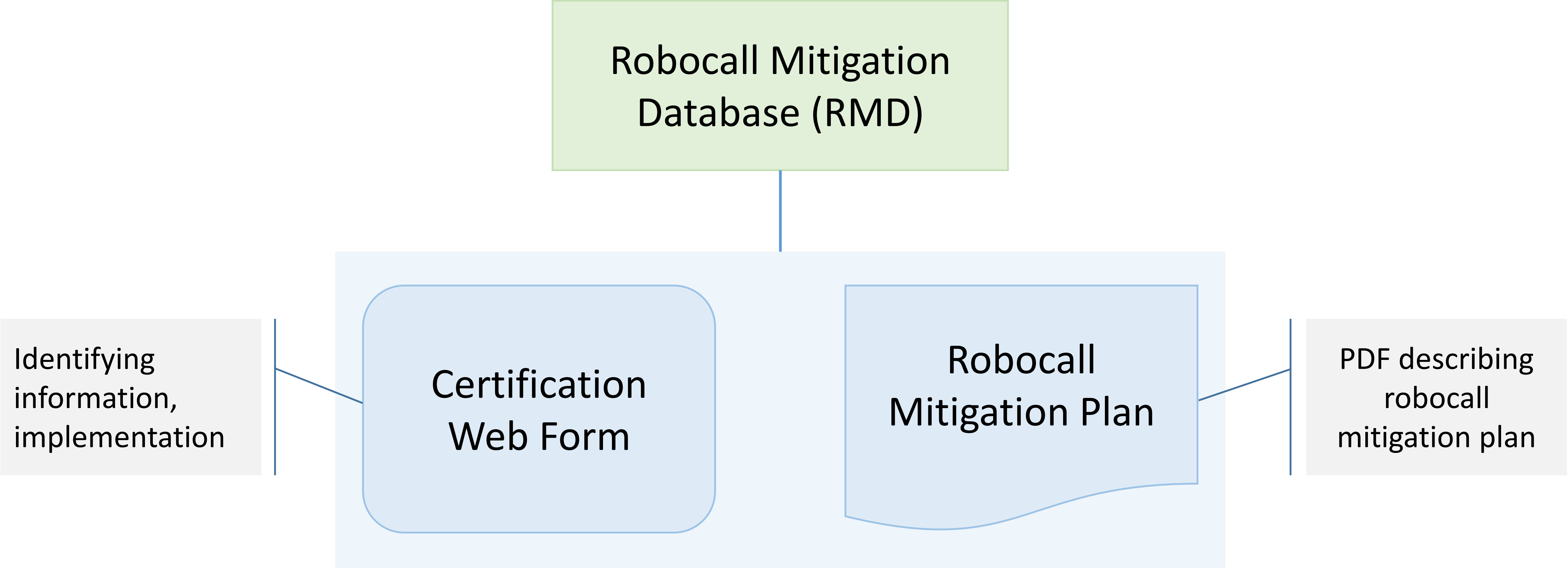
Call analytics examples

- Call volume
- Call duration
- Calls per second
- Calling number invalid, Do-Not-Originate
- Calling number reputation (crowd-sourcing, honey pots…)
- SHAKEN signer reputation (signing robocalls, invalid numbers, improper attestation…)
- Call source or U.S. point of entry
- Subscriber calling number used with an inbound call at the peering NNI

Examples found in legal consent agreements.

Robocall Mitigation Database

All RMD filings will require a certification and a plan



Robocall Mitigation Database (RMD)

Identifying information, implementation

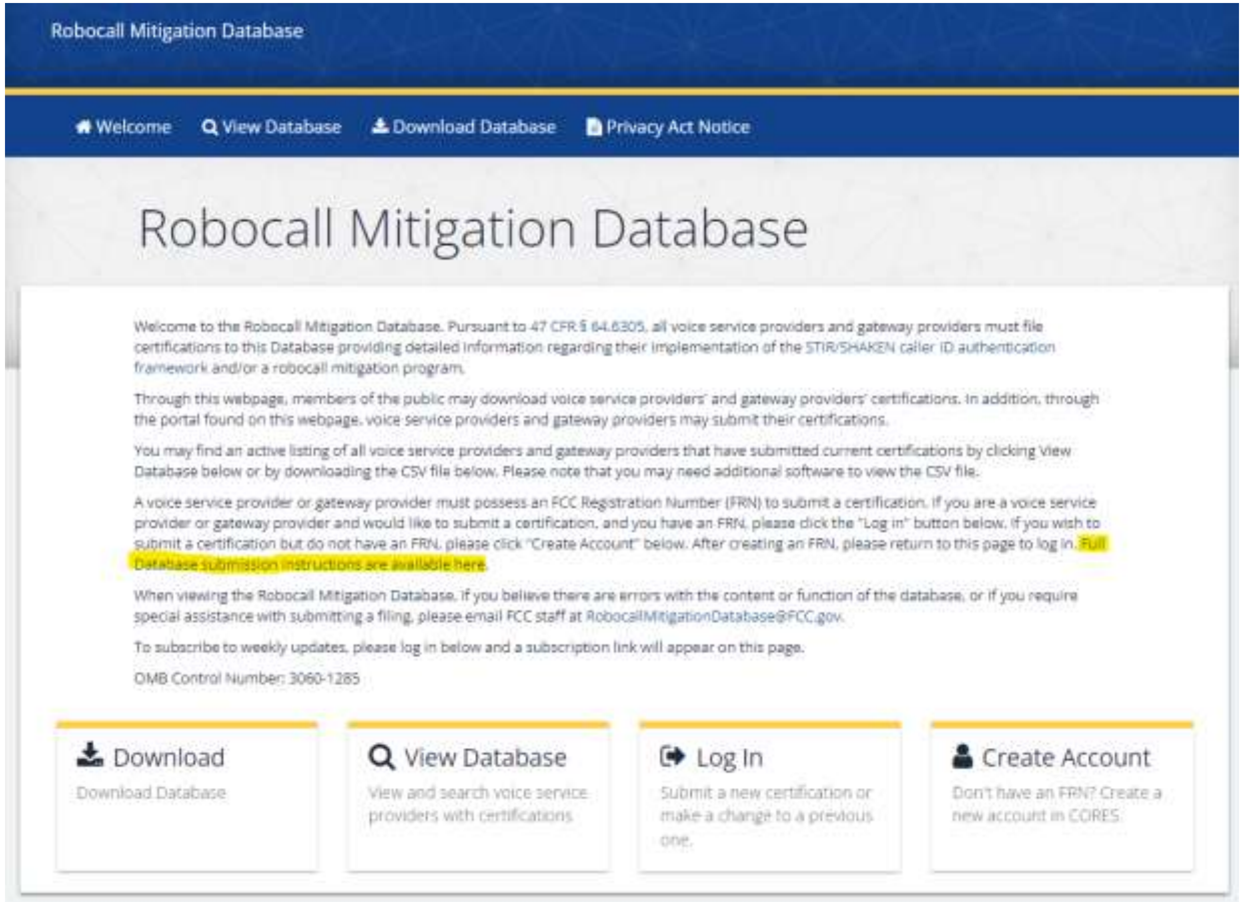
Certification Web Form

Robocall Mitigation Plan

PDF describing robocall mitigation plan

Robocall Mitigation Database access

- Internet search “fcc robocall mitigation database” or
- Click https://fccprod.servicenowservices.com/rmd?id=rmd_welcome
- Instructions are linked on the welcome page, “Full Database submission instructions are available here.”
    - (These instructions are not yet updated for upcoming filing requirements.)
- Use (or create) your CORES login to submit or change your RMD certification.



Robocall Mitigation Database

Welcome to the Robocall Mitigation Database. Pursuant to 47 CFR § 64.6305, all voice service providers and gateway providers must file certifications to this Database providing detailed information regarding their implementation of the STIR/SHAKEN caller ID authentication framework and/or a robocall mitigation program.

Through this webpage, members of the public may download voice service providers' and gateway providers' certifications. In addition, through the portal found on this webpage, voice service providers and gateway providers may submit their certifications.

You may find an active listing of all voice service providers and gateway providers that have submitted current certifications by clicking View Database below or by downloading the CSV file below. Please note that you may need additional software to view the CSV file.

A voice service provider or gateway provider must possess an FCC Registration Number (FRN) to submit a certification. If you are a voice service provider or gateway provider and would like to submit a certification, and you have an FRN, please click the "Log in" button below. If you wish to submit a certification but do not have an FRN, please click "Create Account" below. After creating an FRN, please return to this page to log in. Full Database submission instructions are available here.

When viewing the Robocall Mitigation Database, if you believe there are errors with the content or function of the database, or if you require special assistance with submitting a filing, please email FCC staff at RobocallMitigationDatabase@FCC.gov.

To subscribe to weekly updates, please log in below and a subscription link will appear on this page.

OMB Control Number: 3060-1285

Download
Download Database
View Database
View and search voice service providers with certifications
Log In
Submit a new certification or make a change to a previous one.
Create Account
Don't have an FRN? Create a new account in CORES

New RMD filing requirements

- All providers must file a **plan**
- **Role(s)** in the call chain
- **Exemptions claimed**, with supporting explanation
- **Specific reasonable steps** to mitigate illegal calls
- Affirmative, effective measures to prevent customers from **originating illegal robocalls**
- **Know-Your-Upstream-Provider** procedures
- Certify that the filer has **not been prohibited** from filing in the RMD
- History of **enforcement actions**
- **Call analytics** system(s) used
- **OCN** (Operating Company Number)

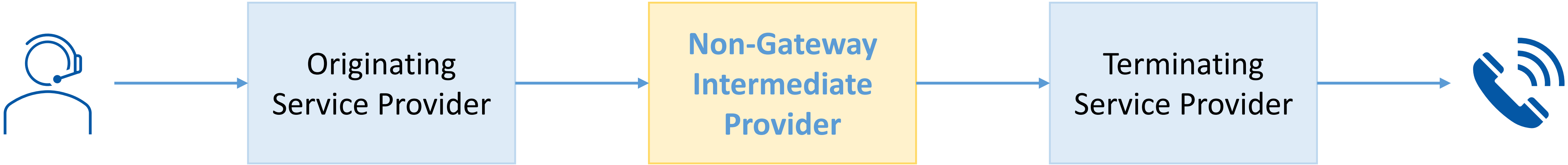
RMD filing deadline

- Requires review by OMB (Office of Management and Budget) for the PRA (Paperwork Reduction Act)
- The Consumer & Government Affairs Bureau and the Wireline Competition Bureau will announce a compliance date after the PRA steps are completed.

STIR/SHAKEN

STIR/SHAKEN by non-gateway intermediate providers

- Effective *December 31, 2023*, the **first** non-gateway intermediate provider in the call chain must authenticate **unauthenticated SIP calls** it receives.



Originating Service Provider

Non-Gateway Intermediate Provider

Terminating Service Provider

- Hint: “The first intermediate provider in the call path may completely avoid the need to authenticate calls if it implements contractual provisions with its upstream originating providers stating that it will **only accept authenticated traffic**.” (Sixth Order ¶ 20)

How do you know if you’re the first NGW Intermediate?

- “Intermediate providers should know whether they receive calls directly from an originating provider pursuant to contracts that provide information to the intermediate provider about the originating provider’s customers and expectations for handling their traffic.” (Sixth Order footnote 74)
- But does this even matter? See hint on previous slide.

Takeaways

- Rules vary by provider role on a call-by-call basis.
  - Know your roles
- Robocall mitigation was initially an *alternative* to STIR/SHAKEN
  - That was a bad idea: call authentication ≠ robocall mitigation
  - Now both will be **mandatory**
- RMD certification and plan requirements will be more substantial
  - Meeting these requirements may be non-trivial for some providers, but do-able
- STIR/SHAKEN by non-gateway intermediates seems intended to force OSPs to authenticate their calls

TransNexus®

- Thank you for attending!
- Robocall mitigation plan template for TransNexus customers
  - Covers many roles—some may not apply to your business
  - Remove what doesn't apply, update what's left
- Robocall mitigation and STIR/SHAKEN solutions
  - Easy compliance
  - Improve service for your customers
  - Contact us to learn more!

info@transnexus.com

(404) 526-6060

transnexus.com