

CARRIER UPGRADE, LLC
1898 South State St, Ste 310 #1190, Orem,
Utah 84097
Tel 202.249.5923
FCC Registration Number (FRN):
0036233260 www.carrierupgrade.org



FEBRUARY 24, 2026

ROBOCALL MITIGATION PLAN

SUMMARY

CARRIER UPGRADE, LLC is a wholesale voice service provider committed to preventing illegal robocalls from originating on, terminating to, or routing through the CARRIER UPGRADE network. This comprehensive robocall mitigation plan describes the reasonable steps CARRIER UPGRADE has implemented to combat illegal robocalls in compliance with Federal Communications Commission regulations and the TRACED Act.

I. CUSTOMER VERIFICATION AND DOCUMENTATION (KNOW YOUR CUSTOMER)

CARRIER UPGRADE, LLC requires each new customer to complete a comprehensive Know Your Customer (KYC) verification process prior to provisioning network connectivity. Our multi-layered approach includes both information collection and independent verification to ensure we do not facilitate illegal robocall traffic.

Information Collected

For all customers, CARRIER UPGRADE collects:

- Full legal name of the company
- All business and trade names, fictitious names, and DBAs for the previous three years
- State or country of incorporation and year of incorporation
- Federal Tax ID (EIN) for U.S. entities or foreign business license number
- Physical address of operations
- Billing name and address (when different from physical address)
- Website address and social media handles
- Contact information for billing, compliance, operations/network, and direct/indirect owners
- Detailed description of business type and voice services provided
- Types of businesses served (customer profile)
- Specific use case for voice service with CARRIER UPGRADE
- Traffic type information (conversational, auto-dialed, telemarketing, U.S. point of entry)
- Anticipated call volumes
- Trade references from other telecommunications carriers
- Regulatory registration information (FRN, FCC 499, FCC 214, RMD status, STIR/SHAKEN implementation)

Independent Verification Procedures

CARRIER UPGRADE does not accept customer-provided information at face value. Each application undergoes independent verification including:

Corporate Identity Verification:

- Federal EIN verification through IRS-issued documentation (CP-575 letter or Form W-9 signed under penalty of perjury)
- Verification of incorporation through state or country business registration records
- For U.S. entities, verification of good standing with state Secretary of State offices where available
- For foreign entities, review of business registration documentation and owner photo identification

Address Verification:

- Physical address validation using USPS address verification to confirm deliverability
- Visual verification via Google Maps to confirm addresses correspond to commercial locations
- For voice service provider customers, cross-referencing addresses against FCC 499 Filer Database and Robocall Mitigation Database registrations
- Assessment of whether residential or virtual office addresses are appropriate for the stated business type and volume

Email and Domain Verification:

- CARRIER UPGRADE requires all business customers to use corporate email domains matching their business name
- Generic email providers (Gmail, Yahoo, Hotmail, etc.) are not accepted for business accounts
- Email domains are verified to match the customer's stated business name and website
- WHOIS lookups are performed to determine domain registration age
- Domains registered less than 90 days prior to application trigger enhanced due diligence review

Website and Online Presence Verification:

- Customer websites are reviewed to confirm they match the stated business purpose
- Website content is assessed for substantive business information versus generic templates
- Website age is verified through WHOIS records and web archive services

Trade Reference Verification:

- Provided trade references are contacted to verify customer payment history and compliance record
- References are verified to be legitimate telecommunications carriers

Regulatory Verification:

- For carrier customers, verification of FCC Registration Number (FRN) against FCC databases
- Verification of FCC Form 499 filing status
- Verification of Robocall Mitigation Database registration and status

Enhanced Due Diligence

Applications receive enhanced scrutiny and additional verification when any of the following risk indicators are present:

- Newly registered businesses (less than 24 months of operation)
- Newly registered website domains (less than 90 days)
- High call volume requests (greater than 10,000 calls per month) inconsistent with stated business size or operating history

- Residential addresses combined with high-volume requests
- Virtual office or mailbox service addresses combined with limited operating history
- Limited or no established online presence
- Inability to provide verifiable trade references from established telecommunications carriers
- Discrepancies between stated business purpose and website content or online presence

Enhanced due diligence procedures include:

- Video conference calls with business principals to verify operations and business model
- Request for detailed business plans and use case documentation
- Review of sample customer contracts or service agreements
- Verification of business bank account information
- Initial call volume caps with gradual increases based on demonstrated compliance

Ongoing Monitoring

Customer verification extends beyond initial onboarding.

Voice Service Provider Customers - Special Requirements

For customers identified as domestic voice service providers, foreign voice service providers, and gateway voice service providers, CARRIER UPGRADE conducts:

- Yearly verification of FCC certification status and Robocall Mitigation Database filing status
- Cross-referencing of customer names and information against FCC Registration Numbers (FRNs), FCC Form 499 filings, and RMD entries
- Immediate termination or suspension of voice service if a voice service provider customer is de-listed from the RMD
- CARRIER UPGRADE refuses to accept traffic from any entity not registered in the RMD, in accordance with 47 CFR § 64.6305(d)

II. KNOW YOUR UPSTREAM PROVIDER

CARRIER UPGRADE maintains detailed information about all upstream voice service providers from whom we receive traffic. Our Know Your Upstream Provider (KYUP) procedures ensure we do not facilitate illegal robocalls from upstream sources.

Upstream Provider Documentation

For each upstream provider, CARRIER UPGRADE collects and maintains:

- Full legal business name and business address
- Nature of business
- FCC Registration Number (FRN)
- FCC Form 499 filing status
- Robocall Mitigation Database registration number and status

Upstream Provider Verification

CARRIER UPGRADE verifies each upstream

provider by confirming active FCC registration and good standing

- Verifying current Robocall Mitigation Database registration status

- Reviewing RMD filing to confirm upstream provider has robocall mitigation procedures
- Checking Industry Traceback Group records for any non-cooperative designations
- Verifying business legitimacy through state registration records where available

Upstream Traffic Refusal Requirements

In compliance with 47 CFR § 64.6305(d), CARRIER UPGRADE refuses to accept traffic from any upstream voice service

provider that:

- Is not registered in the FCC's Robocall Mitigation Database
- Has been removed from the Robocall Mitigation Database
- Has been designated as a non-cooperative provider by the Industry Traceback Group
- Has been notified by the FCC to cease carrying traffic from specific sources

Contractual Provisions

All interconnection agreements with upstream providers include contractual provisions requiring:

- Compliance with all applicable federal and state laws prohibiting illegal robocalls
- Cooperation with all traceback requests from the FCC, law enforcement, and the Industry Traceback Group
- Prohibition on transmitting traffic from sources known or suspected to be generating illegal robocalls
- Right of CARRIER UPGRADE to immediately suspend or terminate service for violations of anti-robocall provisions

Upstream Traffic Monitoring

CARRIER UPGRADE monitors traffic received from upstream providers for patterns consistent with illegal

robocalls, including:

- Sequential called-number dialing patterns
- Calls to known invalid, unallocated, or Do Not Originate numbers
- Spoofed originating numbers

When suspicious patterns are detected from an upstream provider, CARRIER UPGRADE investigates and may suspend traffic from that provider pending resolution.

III. CONTRACTUAL OBLIGATIONS

CARRIER UPGRADE customer service agreements explicitly prohibit the unlawful use of CARRIER UPGRADE network, including the transmission of illegal robocalls.

Anti-Robocall Provisions

All customer contracts include provisions requiring customers to:

- Comply with all applicable international, federal, and state laws and regulations regarding telecommunications, including but not limited to the Telephone Consumer Protection Act (TCPA), Truth in Caller ID Act, Telemarketing Sales Rule (TSR), and state robocall and telemarketing laws
- Refrain from transmitting illegal robocalls, spoofed caller ID information, or other unlawful traffic
- Implement their own robocall mitigation procedures and maintain current Robocall Mitigation Database registration (for voice service provider customers)
- Cooperate fully and promptly with all traceback requests from the FCC, law enforcement, Industry Traceback Group, and CARRIER UPGRADE

Enforcement and Termination

Customer contracts provide that any violation of anti-robocall provisions results in:

- Immediate suspension or termination of service at CARRIER UPGRADE sole discretion
- No refund of prepaid fees or deposits
- Customer liability for any fines, penalties, or damages incurred by CARRIER UPGRADE as a result of customer's illegal activity

Traceback Response Obligations

Customer contracts explicitly stipulate that customers must:

- Respond to traceback requests within 24 hours
- Provide complete and accurate information about call sources
- Take immediate effective steps to stop illegal traffic when identified
- Maintain records sufficient to respond to traceback requests for a minimum of two years

Failure to respond to traceback requests or providing false information is grounds for immediate service termination.

IV. CALL BLOCKING AND ANALYTICS SYSTEMS

CARRIER UPGRADE employs multiple automated systems and analytics tools to identify and block illegal robocalls in real-time.

Do Not Originate (DNO) List Blocking

CARRIER UPGRADE automatically blocks all calls on the Do Not Originate list maintained by the Industry Traceback Group and other industry sources. The DNO list includes:

- Numbers used exclusively for inbound calls
- Invalid numbers that do not conform to the North American Numbering Plan
- Government numbers and other protected number categories

CARRIER UPGRADE DNO blocking system:

- Updates continuously from authoritative DNO sources
- Blocks calls in real-time before they enter the network
- Logs all blocked calls for review

North American Numbering Plan (NANP) Conformance

CARRIER UPGRADE employs rigorous systems to block any originating numbers that do not conform to the North American Numbering Plan, including:

- Invalid area codes
- Invalid exchange codes

Non-compliant numbers are blocked in real-time and logged.

Third-Party Analytics - YouMail

CARRIER UPGRADE utilizes YouMail's commercial robocall analytics

service, which:

- Tracks and analyzes billions of live calls to millions of real consumers
- Identifies phone numbers associated with illegal robocall campaigns
- Provides real-time reputation scoring for originating numbers
- Flags numbers based on consumer complaints and call pattern analysis
- Updates reputation data continuously based on ongoing call activity

CARRIER UPGRADE integrates YouMail data into blocking decisions by automatically blocking numbers flagged by YouMail as SPAM or scam operations.

Federal Trade Commission (FTC) Complaint Data

CARRIER UPGRADE monitors the Federal Trade Commission's Do Not Call (DNC) complaint database and integrates FTC-reported numbers into blocking systems. The FTC publishes complaint data identifying numbers reported by consumers for:

- Violations of the National Do Not Call Registry
- Illegal robocalls and prerecorded messages
- Telemarketing fraud and scam operations
- Caller ID spoofing

Internal Traffic Pattern Analysis

CARRIER UPGRADE conducts continuous analysis of Call Detail Records (CDRs) to identify traffic patterns consistent with illegal robocalling, including:

Volume-Based Indicators:

- Sudden traffic spikes inconsistent with customer's historical patterns or stated business model
- Extremely high call volumes from newly activated customers

Pattern-Based Indicators:

- Short average call duration (under 6 seconds) combined with low answer rates
- Sequential called-number dialing
- Repetitive calling patterns to the same numbers

Customer Suspension: Service is immediately suspended when:

- Customer fails to respond to investigation within 24 hours
- Investigation reveals illegal robocall activity
- Customer is subject to traceback request and fails to cooperate

V. STIR/SHAKEN IMPLEMENTATION

CARRIER UPGRADE, LLC has fully implemented the STIR/SHAKEN call authentication framework on its network to combat caller ID spoofing and verify the authenticity of call signatures.

CARRIER UPGRADE STIR/SHAKEN Configuration

- **Operating Company Number (OCN):** 120L
- **Service Provider Code (SPC) Token:** CARRIER UPGRADE holds its own SPC token issued by the STI-Policy Administrator
- **Certificate Authority:** TELONIUM TELECOMMUNICATIONS LLC
- **Digital Certificate:** CARRIER UPGRADE uses its own digital certificate obtained through TELONIUM TELECOMMUNICATIONS LLC
- **Authentication Authority:** CARRIER UPGRADE makes all attestation-level decisions independently in compliance with third-party authentication requirements effective September 18, 2025 (FCC 24-120)

Call Signing - Originated Traffic

All voice traffic originated on the CARRIER UPGRADE network is signed using the STIR/SHAKEN framework. CARRIER UPGRADE applies attestation levels based on:

A-Level Attestation (Full Attestation):

- CARRIER UPGRADE can verify both the caller's identity and the caller's right to use the calling number
- Applied to calls from customers where CARRIER UPGRADE has verified number ownership or authorization
- Requires documentary evidence of number authorization (LOA, port confirmation, number assignment records)

B-Level Attestation (Partial Attestation):

- CARRIER UPGRADE can verify the caller's identity but not the right to use the specific calling number
- Applied to authenticated customers where number authorization cannot be fully verified
- Used for customers with dynamic number pools or number forwarding arrangements

C-Level Attestation (Gateway Attestation):

- CARRIER UPGRADE can verify neither the caller's identity nor the right to use the calling number
- Applied only to transit traffic from authenticated upstream sources
- Limited use consistent with FCC gateway provider guidelines

CARRIER UPGRADE does not sign calls with attestation levels higher than justified by available verification

information. **Call Verification - Received Traffic**

For calls received from upstream voice service providers, CARRIER UPGRADE verifies STIR/SHAKEN

signatures: **Signature Validation:**

- Each received call with a STIR/SHAKEN signature is validated against the signing certificate
- Certificate validity, expiration, and revocation status are checked in real-time
- Signature integrity is verified to ensure the call has not been altered in transit

Invalid Signature Handling:

- Calls with invalid STIR/SHAKEN signatures are blocked and not permitted to complete

Unsigned Call Handling:

- Unsigned calls from STIR/SHAKEN-capable providers are blocked
- Patterns of unsigned calls from providers required to implement STIR/SHAKEN are reported to upstream providers
- Persistent delivery of unsigned calls when signing is required may result in suspension of upstream interconnection

VI. RESPONDING TO TRACEBACK REQUESTS

CARRIER UPGRADE, LLC is committed to ensuring its network is not utilized for illegal robocalls. CARRIER UPGRADE responds promptly and completely to all traceback requests from the Federal Communications Commission, law enforcement agencies, state attorneys general, and the Industry Traceback Group (ITG).

Traceback Response Commitment

CARRIER UPGRADE will:

- Respond to all traceback requests within 24 hours of receipt
- Provide complete and accurate information about the source of traced calls
- Maintain all records necessary to respond to traceback requests for a minimum of two years, including Call Detail Records, customer agreements, and upstream interconnection records
- Cooperate fully with requesting entities in investigating illegal robocall sources
- Take immediate effective steps to mitigate illegal traffic when identified through traceback

Designated Traceback Contacts

Primary Traceback Contact:

- Name: Support
- Email: contact@carrierupgrade.org

Record Retention

CARRIER UPGRADE maintains records sufficient to respond to traceback

requests including:

- Call Detail Records (CDRs) for all calls: 2 years minimum
 - Customer agreements and KYC documentation: Duration of relationship plus 2 years
 - Upstream provider interconnection agreements: Duration of relationship plus 2 years
-

Enforcement Actions Taken

CARRIER UPGRADE maintains the right to and

does exercise:

- Immediate traffic blocking for DNO, NANP non-conformant, or analytically flagged calls
- Service suspension for customers under investigation
- Service termination for customers confirmed to be transmitting illegal robocalls
- Refusal to accept traffic from de-listed RMD providers
- Termination of upstream interconnections for non-cooperative providers

Plan Updates

This robocall mitigation plan is reviewed and updated:

- Annually as part of RMD recertification requirements
 - Within 10 business days of any material change to mitigation procedures
 - In response to new FCC rules, orders, or enforcement guidance
 - Based on effectiveness assessments and emerging robocall threat patterns
-

Reporting to FCC

CARRIER UPGRADE will comply with all

requirements to:

- Report to the FCC Enforcement Bureau when CARRIER UPGRADE identifies customers transmitting illegal robocall traffic
 - Provide information to the FCC upon request regarding robocall mitigation efforts
 - Update RMD filing within 10 business days of material changes to contact information or mitigation procedures
 - Maintain accurate and current information in all FCC databases including CORES, Form 499, and RMD
-

VIII. CONCLUSION

CARRIER UPGRADE, LLC is committed to robust robocall mitigation practices that protect consumers from illegal and unwanted robocalls. Through comprehensive Know Your Customer verification, Know Your Upstream Provider procedures, advanced analytics and blocking systems, full STIR/SHAKEN implementation, prompt traceback cooperation, and contractual enforcement, CARRIER UPGRADE takes all reasonable steps to prevent its network from being used for illegal robocall traffic.

CARRIER UPGRADE will continue to cooperate with the Federal Communications Commission, law enforcement, state attorneys general, the Industry Traceback Group, and other regulatory bodies to create a secure telecommunications environment and combat the negative impacts of illegal robocalls on American consumers.

Certification:

The undersigned certifies that the information provided in this Robocall Mitigation Plan is true, accurate, and complete to the best of their knowledge. The undersigned has authority to bind CARRIER UPGRADE, LLC and certifies that CARRIER UPGRADE will comply with all requirements of this plan and all applicable FCC regulations regarding robocall mitigation.

Name: KARTIK BAWA

Title: ceo

Date: 2/24/2026