

Porting.com, LLC d/b/a NumHub

Robocall Mitigation Program

Version 1.1 – March 2026

Company Role & Scope

Porting.com, LLC d/b/a NumHub (“NumHub” or “Company”) operates as a non-facilities-based reseller and telecommunications platform provider. NumHub does not operate its own voice network and does not directly originate, terminate, or transport voice traffic.

All call traffic enabled through NumHub’s platforms is carried exclusively by underlying FCC-authorized carrier partners, including but not limited to Teliax, Inc., who are responsible for call routing, interconnection, and STIR/SHAKEN signing and verification.

NumHub’s role is limited to:

- Customer onboarding and authorization
- Number provisioning and porting management
- Policy enforcement and compliance controls
- Coordination with underlying carriers for enforcement actions

STIR/SHAKEN Implementation

In accordance with 47 C.F.R. §64.6301, STIR/SHAKEN authentication and verification is performed by NumHub’s underlying carrier partners. NumHub requires, by policy, that all carrier partners:

- Fully implement STIR/SHAKEN
- Sign and verify traffic where required
- Maintain active Robocall Mitigation Database (RMD) filings

ROBOCALL MITIGATION PROGRAM

Regulatory Basis

This Robocall Mitigation Program (“RMP”) is submitted pursuant to:

- 47 C.F.R. §64.6305(a)(1) and (d)(5)
- FCC Sixth Report and Order, WC Docket No. 17-97 (March 17, 2023)

Commitment to Traceback Cooperation

NumHub commits to:

- Respond within 24 hours to all traceback requests from:
 - FCC

- Law Enforcement
- Industry Traceback Group (ITG)
- Coordinate directly with its underlying carrier partners to:
 - Identify the responsible customer
 - Investigate traffic sources
 - Enforce corrective actions, including suspension or termination

Traceback Contact

Title: Compliance & Network Operations

Email: orders@numhub.com

Traceback Handling Process

1. Receive traceback request
2. Identify customer and number(s) involved
3. Coordinate with underlying carrier(s)
4. Suspend or restrict customer if necessary
5. Respond to requesting authority within 24 hours

Call Monitoring & Analytics

NumHub does not inspect or route live call traffic. However, NumHub:

- Requires its carrier partners to perform:
 - Traffic analytics
 - DNO/DNC filtering
 - Pattern and velocity detection
- Receives:
 - Exception reports
 - Abuse notifications
 - Compliance alerts

Based on these, NumHub may:

- Suspend a customer
- Block number provisioning
- Revoke number authorization

- Terminate the account

Know Your Customer (KYC) Program

NumHub enforces strict onboarding requirements:

Customers must provide:

- Legal entity name
- Incorporation jurisdiction
- Physical address
- EIN
- Business description and use case
- Authorized signatory

If the customer is a Voice Service Provider or traffic aggregator:

- NumHub verifies their FCC RMD listing before enabling service

Additional controls:

- Risk scoring at onboarding
- Enhanced review for higher-risk use cases
- Annual re-validation

Validation of Right to Use Numbers

NumHub only allows:

- Numbers assigned by NumHub
- Numbers ported into NumHub
- Numbers explicitly authorized by the legal owner

All numbers are:

- Tracked in inventory systems
- Bound to customer accounts
- Governed by caller ID authorization rules

Unauthorized usage results in immediate suspension.

Accepting Traffic From Other Providers

NumHub itself does not accept traffic.

However, NumHub requires all underlying carrier partners:

- Only exchange traffic with providers listed in the FCC RMD
- Follow all 47 C.F.R. §64.6305(e) requirements

Emergency Services

NumHub does not block or interfere with:

- 911 calls
- PSAP traffic
- Emergency services traffic

Acceptable Use Policy

Customer agreements will explicitly prohibit:

- Robocalling
- Spoofing
- Fraud
- Illegal telemarketing
- Any traffic violating FCC, FTC, or TCPA rules

NumHub reserves the right to:

- Immediately suspend service
- Disable number access
- Terminate customer relationships
- Refer matters to law enforcement or carriers

Conclusion

NumHub submits this Robocall Mitigation Plan as a non-facilities-based reseller that does not originate, terminate, or transport calls, and fulfills its compliance obligations through:

- Customer governance
- Number authorization control
- Carrier partner enforcement
- Traceback cooperation

NumHub will update its RMD filing within 10 business days of any material change.