

Robocall Mitigation Program Description

Provider: UMG Systems LLC / Unparallel Media Group

Provider type: Voice service reseller / managed communications provider. UMG does not operate an independent public switched telephone network carrier network and relies on authorized upstream voice carrier(s) for PSTN interconnection, numbering, and STIR/SHAKEN call authentication support, except where UMG may directly control customer account provisioning, acceptable-use enforcement, call handling configuration, and customer support.

Purpose: This program describes the reasonable steps UMG uses to prevent, detect, investigate, and mitigate illegal robocalls and spoofed traffic associated with services it provides or manages.

Version: 2026-05-29. Replace bracketed fields below before filing if any details differ.

1. Scope of Services

UMG provides hosted voice, communications, and related managed services to business customers. UMG may provision users, telephone numbers, extensions, call routing, IVR/auto-attendant features, SIP credentials, and customer account settings through one or more upstream voice platforms or carriers. UMG does not knowingly permit customers or users to originate illegal robocalls, transmit fraudulent caller ID, or use its services for unlawful calling campaigns.

2. STIR/SHAKEN and Upstream Carrier Controls

- UMG relies on upstream voice carrier(s) and platform provider(s) for STIR/SHAKEN implementation, certificate management, caller ID authentication, traceback cooperation, and PSTN interconnection where those functions are outside UMG direct control.
- UMG routes outbound PSTN traffic only through providers that represent compliance with applicable FCC robocall mitigation, call authentication, and traceback obligations.
- UMG does not intentionally alter caller ID information to misrepresent the originating party. Customer caller ID configuration is limited to numbers assigned to, ported by, or otherwise authorized for that customer account.
- Where UMG controls provisioning, it restricts caller ID use to verified or authorized numbers and removes or disables caller ID settings that appear unauthorized, misleading, or abusive.

3. Customer Vetting and Account Controls

- UMG provides service only to identifiable business customers and maintains customer account records, billing contacts, service locations, and responsible administrative contacts.
- UMG may request business identity information, service address, authorized users, number ownership/authorization evidence, and intended use of service when onboarding or changing service.
- UMG prohibits use of its services for unlawful robocalling, spoofing, fraud, impersonation, harassment, traffic pumping, or other abusive calling activity through its customer terms, service policies, or acceptable-use enforcement practices.
- UMG may suspend, restrict, or terminate service when a customer fails to cooperate with an investigation or when UMG identifies credible evidence of illegal robocalling or caller ID abuse.

4. Traffic Monitoring and Abuse Detection

UMG monitors for signs of abusive or suspicious calling using account-level review, customer support reports, upstream provider alerts, traceback requests, complaint notices, abnormal calling patterns, and other available operational indicators. Because UMG may operate as a reseller or managed service provider rather than a facilities-based carrier, certain network analytics may be performed by upstream providers. UMG cooperates with those providers and uses the information available to it to identify and mitigate suspected illegal traffic.

- Examples of suspicious indicators include unusual outbound call volume, high short-duration call ratios, repeated unanswered calls, complaints, invalid or unauthorized caller ID, newly created accounts with high-volume outbound activity, traceback notices, and upstream carrier alerts.
- When suspicious activity is detected, UMG may investigate the customer account, verify the calling purpose, review caller ID authorization, restrict outbound calling, disable affected credentials, remove unauthorized caller ID, require customer remediation, or suspend/terminate the service.

5. Response to Traceback, Enforcement, and Provider Notices

- UMG will cooperate in good faith with traceback requests, upstream carrier investigations, law enforcement requests, FCC-related inquiries, and other lawful requests related to suspected illegal robocalls.
- UMG maintains contact points capable of receiving robocall mitigation or abuse notices and will route such notices to responsible personnel for review and action.
- UMG will provide responsive information available in its records, subject to applicable law and privacy/security limitations.
- UMG will take prompt action when credible evidence indicates that traffic associated with its service is illegal, abusive, spoofed, or otherwise violates applicable rules or policies.

6. Number and Caller ID Authorization

- UMG provisions telephone numbers only where numbers are assigned, ported, delegated, or otherwise authorized for the relevant customer.
- Customer requests to change outbound caller ID may be reviewed for business justification and number authorization.
- UMG will remove, block, or correct caller ID configurations that appear unauthorized, misleading, spoofed, or inconsistent with customer authorization records.

7. Remediation Measures

Depending on the severity, repeat nature, and credibility of the evidence, UMG may apply one or more mitigation actions:

- Customer warning and request for explanation or documentation.
- Temporary outbound calling limits or call blocking on affected users, trunks, numbers, or accounts.
- Password/API/SIP credential reset or disabling of compromised endpoints.
- Removal or correction of unauthorized caller ID settings.
- Suspension or termination of service for confirmed or unresolved abusive activity.
- Escalation to the upstream carrier, platform provider, or appropriate legal/enforcement contact.

8. Recordkeeping and Review

- UMG maintains commercially reasonable records relating to customer accounts, assigned numbers, service configuration, support tickets, abuse reports, remediation actions, and provider notices.
- UMG reviews its robocall mitigation practices periodically and updates this program when services, upstream providers, regulations, or operational controls materially change.
- UMG will update its Robocall Mitigation Database filing within the required timeframe when filing information, certification information, contact information, or this mitigation program materially changes.

9. Certification Statement Placeholder

The undersigned certifies, under penalty of perjury and consistent with applicable FCC requirements, that the information submitted in connection with this Robocall Mitigation Program Description is accurate and that UMG Systems LLC is taking reasonable steps described above to avoid originating, carrying, or enabling illegal robocall traffic through services within its control.

Authorized officer:	[Name / Title]
Company:	UMG Systems LLC
Date:	[Date]
Email:	[Compliance email]
Phone:	[Compliance phone]

Filing note

Before uploading, confirm the exact provider type, FRN, contact information, upstream provider names if required by the FCC form, and whether UMG has any direct originating, intermediate, gateway, or foreign-provider role beyond reseller/managed-service functions. Do not certify facts that are not true for the provider.