

ROBOCALL MITIGATION PROGRAM DESCRIPTION

TELEflash GmbH

Foreign Voice Service Provider - Germany

Prepared for filing in the Federal Communications Commission
Robocall Mitigation Database

Version 1.0 | Effective September 25, 2026

Filing entity	TELEflash GmbH
Provider type	Foreign Voice Service Provider
STIR/SHAKEN status	No current TELEflash STIR/SHAKEN implementation; foreign provider without a domestic implementation obligation
Document purpose	Public description of specific reasonable steps used to prevent the origination of illegal robocall traffic

This description is intended to explain TELEflash GmbH's robocall mitigation program at a level sufficient to identify the specific controls used, while avoiding disclosure of exact security thresholds, fraud rules, credentials, or other operational parameters that could facilitate circumvention of those controls.

1. Purpose and Scope

TELEflash GmbH ("TELEflash") is a German telecommunications and Voice over IP service provider. This Robocall Mitigation Program describes the affirmative and effective measures TELEflash uses to reduce the risk that its network or services are used to originate illegal robocalls or calls using misleading or unauthorized caller identification.

The program applies to voice traffic originated by TELEflash customers and to the systems, personnel, customer onboarding procedures, contractual controls, traffic analytics, escalation processes, and carrier-management procedures used to deliver that traffic. TELEflash reviews the effectiveness of the program and adjusts controls in response to observed abuse patterns, traceback information, carrier feedback, regulatory developments, and changes in its services.

This program is designed to satisfy the requirements applicable to voice service providers under 47 CFR § 64.6305 and the obligation in 47 CFR § 64.1200(n)(4) to take affirmative, effective measures to prevent new and renewing customers from using the network to originate illegal calls, including knowing customers and exercising due diligence to prevent illegal traffic.

2. Regulatory and Compliance Framework

TELEflash operates primarily under German and European telecommunications and data-protection law while also complying with applicable U.S. obligations for traffic that terminates in the United States.

2.1 United States requirements

- 47 CFR § 64.6305: robocall mitigation program, RMD certification, specific reasonable mitigation steps, analytics disclosure, and traceback cooperation.
- 47 CFR § 64.1200(n)(4): affirmative, effective measures for new and renewing customers, including customer identification and due diligence designed to prevent illegal call origination.
- Truth in Caller ID Act / 47 CFR § 64.1604: prohibition on transmitting misleading or inaccurate caller identification information with intent to defraud, cause harm, or wrongfully obtain anything of value.

2.2 German and European framework

- German Telecommunications Act (Telekommunikationsgesetz - TKG), including § 120 concerning caller-number transmission and authorization to use caller numbers, and § 165 concerning appropriate technical and organizational safeguards for telecommunications networks and services.
- German Telecommunications-Digital-Services Data Protection Act (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz - TDDDG), including telecommunications secrecy and lawful handling of traffic data.
- Regulation (EU) 2016/679 (GDPR), in particular Articles 5 and 6 concerning lawful, purpose-limited and data-minimized processing, and Article 32 concerning appropriate security of processing.

TELEflash applies these requirements in a manner intended to preserve telecommunications confidentiality and data-protection rights while permitting proportionate fraud prevention, network security, billing, abuse investigation, and compliance activities.

3. Know-Your-Customer and Customer Qualification

TELEflash does not provide unrestricted anonymous access to outbound voice origination. Before activating voice services, and again when a customer relationship is materially changed or renewed, TELEflash performs risk-based customer qualification appropriate to the customer type, requested services, expected traffic profile, requested numbering resources, and anticipated call volume.

3.1 Business customer verification

For business customers, TELEflash normally collects and verifies a combination of the following information, as appropriate to the risk presented:

- full legal company name, legal form, registered address, business address, and billing address;
- commercial-register or equivalent company-registration information and, where applicable, VAT identification information;
- identity and authority of the person acting for the customer, including confirmation that the individual is authorized to enter into the service relationship;
- business-domain email address and working contact information;
- the nature of the customer's business, intended use of the voice service, anticipated geographic calling patterns, expected traffic volume, and requested numbering resources;
- payment and account information sufficient to identify inconsistencies or elevated fraud risk; and

-
- additional supporting documents where the information supplied is incomplete, inconsistent, unusual, or the customer seeks high-volume origination capability.

Where appropriate, TELEflash corroborates supplied information against reliable external sources such as official commercial/company registers, VAT-validation resources, public corporate information, or other independent sources. Higher-risk or high-volume applicants are subject to enhanced review before service is activated or limits are increased.

3.2 Customer risk indicators and enhanced due diligence

Examples of circumstances that may result in additional review, delayed activation, lower initial limits, or rejection include:

- inconsistent company, address, identity, payment, or contact information;
- a newly created or unverifiable business identity that does not reasonably correspond to the requested calling activity;
- requests for unusually high call concurrency or volume without a credible business justification;
- requests to transmit caller IDs that cannot be associated with the customer or verified as authorized;
- unusual geographic discrepancies between the customer, technical access points, payment information, and stated business operations;
- prior abuse complaints, carrier warnings, traceback history, or other credible indicators of illegal or abusive calling.

TELEflash may refuse activation or terminate a relationship where customer identity, authority, or intended use cannot be satisfactorily established.

3.3 Renewal and ongoing customer review

Customer qualification is not limited to the initial sign-up. TELEflash re-evaluates customer risk when material account information changes, when significant new services or capacity are requested, when traffic behavior materially departs from the established profile, when abuse complaints or traceback requests are received, or when other information indicates that the original risk assessment may no longer be reliable.

4. Contractual and Acceptable-Use Controls

TELEflash service terms and operational policies prohibit customers from using TELEflash services for unlawful, fraudulent, deceptive, abusive, or unauthorized calling. Contractual and operational controls are designed to permit prompt intervention where abuse is detected.

The applicable customer obligations include, as appropriate:

- no use of TELEflash services to originate illegal robocalls, scam calls, fraudulent calls, or calls that violate applicable telemarketing or consumer-protection law;
- no caller-ID spoofing or presentation of numbers for which the customer lacks a legitimate right of use;
- customers must maintain accurate account and contact information and respond to reasonable compliance or abuse inquiries;
- customers must cooperate with investigations of suspected unlawful traffic and provide information reasonably necessary to validate calling activity;
- TELEflash may impose limits, block specific traffic, suspend origination, restrict caller IDs, or terminate services where there is credible evidence of abuse or material non-compliance.

5. Caller-ID and Number Authorization Controls

Caller-ID integrity is a central control in TELEflash's mitigation program. TELEflash applies technical and administrative controls intended to prevent customers from freely presenting arbitrary caller numbers.

Depending on the service configuration, outbound caller identification is limited to numbers that are:

- assigned by TELEflash or a partner carrier for the customer's use;
- ported to the customer or otherwise associated with the customer; or
- independently verified as a number the customer is authorized to use.

TELEflash may reject, normalize, suppress, or otherwise restrict caller-ID values that do not satisfy the applicable authorization rules. For German numbering, TELEflash also observes the caller-number transmission principles in § 120 TKG. For U.S. numbering used by TELEflash customers, TELEflash maintains sufficient account records to support validation of the customer's authorization to use the number and to respond to carrier or traceback inquiries.

6. Network Analytics, Rate Controls, and Automated Blocking

TELEflash operates intelligent, rule-based and behavioral controls designed to detect calling patterns that are inconsistent with the customer's authorized service profile or are characteristic of automated abuse. These controls operate at the network and account level and are complemented by manual investigation when appropriate.

6.1 Call-rate and velocity controls

- per-account and per-trunk call-per-second and call-rate controls;
- concurrent-call limits and burst controls;
- rate controls that can be adjusted according to customer risk, service type, history, and approved traffic profile;
- automatic throttling, rejection, or blocking where configured risk thresholds are exceeded.

6.2 Behavioral and anomaly detection

TELEflash evaluates traffic characteristics that may indicate abnormal automated calling. Depending on context, indicators can include:

- sudden increases in call volume or concurrency inconsistent with historical behavior;
- large-scale sequential or highly repetitive dialing patterns;
- unusual destination concentration or rapid geographic changes;
- abnormally high proportions of very short calls, failed calls, rejected calls, or other signaling patterns associated with abusive campaigns;
- repeated use or rotation of caller IDs inconsistent with the customer's assigned or verified number inventory;
- traffic that materially deviates from the use case, expected hours, geographic footprint, or volume approved during onboarding;
- credible abuse reports, traceback notifications, carrier complaints, or other external indicators correlated with the observed traffic.

The controls are designed to support proportionate intervention rather than indiscriminate blocking. Exact thresholds and fraud-scoring parameters are confidential operational security values and are not published because disclosure could enable evasion.

6.3 Response actions

When automated systems or staff identify suspicious activity, TELEflash may take one or more of the following actions based on severity and confidence:

- apply additional rate or concurrency limits;
- block specific destination patterns or caller IDs;
- temporarily suspend outbound origination;
- require re-verification of customer identity, number authorization, or business purpose;
- request supporting documentation concerning the calling campaign or traffic source;
- terminate the service relationship for confirmed or material abuse;
- preserve and provide relevant records when lawfully required for traceback, regulatory, or law-enforcement cooperation.

6.4 Analytics systems and vendors

The mitigation controls described above are implemented within TELEflash's own network, provisioning, rating, and operational control environment. TELEflash does not rely solely on downstream carrier screening to prevent illegal traffic. Any security, fraud-prevention, or reputation information received from interconnecting carriers is treated as supplemental input to TELEflash's own controls.

At the time of this program description, TELEflash does not use a dedicated third-party robocall analytics vendor for the origination analytics described above. If a dedicated third-party analytics vendor is introduced, TELEflash will update its Robocall Mitigation Database information as required.

7. Know-Your-Upstream-Provider Procedures

Where TELEflash receives voice traffic, numbering services, or PSTN interconnection from another provider, TELEflash performs proportionate due diligence on the provider relationship. Depending on the service and jurisdiction, this includes review of the provider's legal identity, service-provider status, technical and abuse contacts, contractual responsibilities, relevant regulatory standing, and ability to support traceback and abuse investigation.

For U.S.-related voice interconnection, TELEflash checks whether an upstream or directly interconnected provider is appropriately listed in the FCC Robocall Mitigation Database where such listing is required and seeks contractual and operational arrangements that permit cooperation on illegal-call mitigation, traceback, caller-ID integrity, and suspension or blocking of abusive traffic.

TELEflash avoids knowingly establishing or maintaining interconnection arrangements with providers that refuse reasonable compliance cooperation or present unresolved indications of repeated facilitation of illegal robocall traffic.

8. Continuous Monitoring and Incident Handling

TELEflash monitors network and account-level indicators on an ongoing basis. Alerts and anomalies are reviewed according to severity. Where suspicious traffic is identified, TELEflash correlates technical records with customer account information, caller-ID authorization, traffic history, and any external complaint or traceback information.

The purpose of this process is to identify the responsible customer or traffic source rapidly, stop or restrict problematic traffic, and preserve sufficient information to support carrier, regulatory, or law-enforcement investigation. TELEflash may escalate accounts for enhanced monitoring after an incident even where immediate termination is not warranted.

9. Traceback and Regulatory Cooperation

TELEflash commits to respond fully and within 24 hours to traceback requests from the Federal Communications Commission, U.S. law enforcement, and the designated industry traceback consortium, and to cooperate with those entities in investigating and stopping illegal robocallers that use TELEflash's services to originate calls.

TELEflash maintains operational records reasonably necessary to identify the relevant customer or interconnection path, subject to applicable German and European data-protection and telecommunications-confidentiality requirements. Traceback requests are escalated to personnel authorized to investigate the traffic, preserve relevant records, contact the customer or carrier when appropriate, and implement blocking, suspension, or termination measures.

Where a traceback or credible complaint identifies confirmed or suspected illegal traffic, TELEflash will take appropriate remedial steps, which may include immediate traffic restriction, customer re-verification, account suspension, termination, or coordination with the relevant upstream/downstream carrier.

10. Data Protection, Telecommunications Confidentiality, and Record Handling

TELEflash performs robocall mitigation in a manner intended to remain consistent with German and European privacy and telecommunications-confidentiality requirements. Customer-identification and abuse-prevention data are collected for defined operational, contractual, security, fraud-prevention, and legal-compliance purposes and are limited to information reasonably necessary for those purposes.

TELEflash applies the principles of lawfulness, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality under the GDPR. Telecommunications content and traffic information are handled subject to the TDDDG and other applicable laws. Access to compliance and traffic records is restricted to personnel with a legitimate operational or legal need, and technical and organizational security measures are applied consistent with § 165 TKG and Article 32 GDPR.

TELEflash does not use robocall mitigation as a basis for indiscriminate inspection of call content. The program primarily relies on account information, signaling data, caller-ID authorization, traffic metadata, behavioral patterns, complaints, traceback information, and other information that may lawfully be processed for provision, security, fraud prevention, billing, or compliance purposes.

11. Governance, Review, and Updates

Responsibility for the program is assigned to TELEflash management and designated technical/compliance personnel. The program is reviewed periodically and when material events warrant, including significant changes in services, traffic patterns, U.S. regulatory requirements, interconnection arrangements, analytics capabilities, or observed abuse methods.

TELEflash will update its Robocall Mitigation Database filing within the time required by FCC rules when information required to be maintained in the filing materially changes. TELEflash also performs the applicable annual RMD recertification.

12. STIR/SHAKEN Status

TELEflash is a foreign voice service provider organized and operating in Germany. At the date of this description, TELEflash has not implemented STIR/SHAKEN on its own network and is filing as a foreign voice service provider without a domestic STIR/SHAKEN implementation obligation. TELEflash may evaluate voluntary STIR/SHAKEN participation in the future. Any future implementation will be reflected accurately in the RMD filing.

Regardless of STIR/SHAKEN implementation status, all calls originated through TELEflash are subject to this robocall mitigation program.

13. Summary of Specific Mitigation Measures

Control Area	TELEflash Measure
Customer qualification	Verify legal identity, company information, authorized representative, service purpose, and contact/payment consistency; enhanced review for higher-risk or high-volume customers.
Caller-ID authorization	Restrict outbound caller IDs to assigned, ported, or otherwise verified numbers; reject or restrict unauthorized caller-ID use.
Rate controls	Per-account/trunk call-rate, burst, concurrency, and traffic-profile controls with automated throttling or blocking.
Behavioral analytics	Detect material traffic anomalies, repetitive/sequential dialing, suspicious short-call/failure patterns, caller-ID rotation, and deviations from expected use.
Contract controls	Prohibit illegal calls, fraud, unauthorized spoofing and abusive automation; allow immediate restriction, suspension, or termination.
Ongoing monitoring	Review alerts, complaints, carrier feedback, traceback information, and customer traffic changes; re-verify higher-risk customers when needed.
Upstream due diligence	Review interconnecting providers and U.S. RMD status where applicable; require operational cooperation on abuse and traceback.
Traceback	Respond fully within 24 hours to FCC, law-enforcement, and industry traceback consortium requests and cooperate to stop illegal traffic.
Privacy/security	Apply GDPR, TDDDG, TKG and appropriate technical/organizational security measures while limiting processing to legitimate purposes.

14. Commitment

TELEflash is committed to preventing its services from being used to originate illegal robocalls and to maintaining controls that are proportionate to the risks presented by its customer base and services. TELEflash will investigate credible indications of abuse, take prompt remedial action, cooperate with traceback and enforcement requests, and refine its mitigation program as threats, technologies, and regulatory requirements evolve.

Appendix A - Key Legal and Regulatory References

47 CFR § 64.6305: Robocall mitigation and certification requirements.

47 CFR § 64.1200(n)(4): Affirmative, effective measures to prevent new and renewing customers from using a network to originate illegal calls; KYC and due diligence.

47 CFR § 64.1604: Prohibition on misleading or inaccurate caller identification with intent to defraud, cause harm, or wrongfully obtain value.

FCC, Robocall Mitigation Database Frequently Asked Questions for Filers (updated Jan. 20, 2026): Current RMD filing guidance, including foreign-provider filing guidance.

Telekommunikationsgesetz (TKG) §§ 120 and 165: Caller-number transmission and technical/organizational security requirements in Germany.

Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), including §§ 3 and 9: Telecommunications secrecy and traffic-data handling.

Regulation (EU) 2016/679 (GDPR), Articles 5, 6 and 32: Data protection principles, lawful processing, and security of processing.

This document is prepared as the public robocall mitigation program description accompanying TELEflash GmbH's FCC Robocall Mitigation Database filing. It should be updated whenever the controls or facts described above materially change.