

Robocall Mitigation Program

CREATECH INFORMATION TECHNOLOGIES (PRIVATE) LIMITED

Doing business as CallEazy

FCC Registration Number (FRN): 0038979332

Document and effective date: October 6, 2026

Program owner and robocall-mitigation contact: Fawad Anwar, CEO

Email: fawad@createchagency.com

Telephone: +92 315 9585665

1. Company and service

CREATECH INFORMATION TECHNOLOGIES (PRIVATE) LIMITED (the "Company") is a Pakistan-organized foreign voice service provider operating under the CallEazy trade name. CallEazy provides application-based voice service to end users and uses wholesale carriers to connect calls to the public switched telephone network. The Company does not permit customers to upload calling lists, run predictive or unattended dialling campaigns, or select arbitrary calling-line identity through the CallEazy application.

The Company has not implemented the STIR/SHAKEN authentication framework on any portion of a network it controls. Pursuant to 47 CFR § 64.6305(d)(2)(i), the Company explains that it lacks control over the wholesale carrier network infrastructure necessary to implement STIR/SHAKEN. It relies on the wholesale carrier that receives a call for public-network termination to perform any caller-ID authentication applicable to that carrier's controlled network. This allocation must be confirmed with the carrier before the Company submits its certification. This program describes the reasonable steps the Company takes to avoid originating illegal robocall traffic, investigate suspected abuse, cooperate with traceback requests, and stop illegal traffic that uses its service.

2. Governance and responsibility

The CEO is responsible for this program. The CEO or a specifically delegated employee will:

1. monitor the compliance mailbox and telephone contact;
2. review traffic alerts and complaints;
3. investigate suspicious accounts and calls;
4. suspend access and request carrier-level blocking where appropriate;
5. preserve records relevant to complaints and traceback requests; and
6. review this program after a material service, carrier, regulatory, or threat change and at least annually.

The Company will update its Robocall Mitigation Database filing within the period required by FCC rules when filed information materially changes.

3. Customer onboarding and access controls

CallEazy requires an account tied to a syntactically valid E.164-format telephone number and a verified one-time password delivered to the account email address. OTP issuance and verification attempts are rate-limited. The service records the account identity, contact information, account creation time, and relevant device/session information.

CallEazy does not represent this basic account verification as government-identity verification. Where a number category or country

requires enhanced verification, the purchase is blocked until the required records are supplied. The current enhanced rule for German IDT numbers requires an address owned by the account and a passport or driver's-license document before an order can be placed. Requirements are maintained by number category and jurisdiction as carrier requirements are confirmed.

The Company may request additional identity, business-purpose, source-of-funds, or intended-traffic information when an account, purchase, complaint, or traffic pattern presents elevated risk. Failure to provide satisfactory information is grounds to deny service or suspend the account.

4. Caller-ID and number controls

Customers cannot enter an arbitrary originating caller ID in the CallEazy calling flow. For each outbound call, the platform derives the originating number from an active number assigned to and owned by the authenticated account. The server verifies that the selected number belongs to that account. For calls using the Company's current SIP/IDT flow, the platform uses the assigned DID as the From number and records that number with the call.

Destination telephone numbers are subject to a format check consistent with the E.164 maximum length. The platform rejects a call to the same number being used as the originating DID and permits only one active call per account in the current SIP calling flow. Wholesale-carrier requirements for From and P-Asserted-Identity headers are applied at the SIP interconnection. The Company will not knowingly originate a call with a caller ID that the customer is not authorized to use.

5. Traffic controls and monitoring

CallEazy uses prepaid controls. A call is not authorized unless the account has enough wallet value or calling allowance for the initial charge. During SIP calls, usage is charged incrementally. If funds are insufficient, the platform instructs the client to end the call and also requests server-side termination. A background process provides an additional termination and billing backstop. The legacy provider calling flow also calculates a balance-based maximum duration and applies a safety cap.

The administration system provides account-level call-history search and rule-based anomaly review. The current rules surface, among other indicators:

- at least 50 outbound calls shorter than 10 seconds within the selected review period;
- three or more failed transactions within the selected review period;
- five or more eSIM purchases within the selected review period;
- a completed wallet top-up of at least USD 500 combined with fewer than five calls and fewer than five messages during the review period;
- multiple refunds; and
- related-account indicators based on repeated non-public email domains.

These indicators support human review; they are not treated as proof of wrongdoing. Reviewers may also examine destination concentration, call frequency, duration, account age, payment history, device count, complaints, and carrier reports. The Company will adjust thresholds or add controls as traffic volume and observed abuse patterns change.

Number purchases in the current IDT flow are limited to three qualifying

purchases per account in a rolling 24-hour period and require sufficient prepaid funds before a carrier order is placed.

6. Complaints, investigation, and mitigation

Reports concerning suspected illegal robocalls or spoofing are escalated to the program owner. The review will correlate, as available, the calling number, called number, date and time (including time zone), provider call identifier, CallEazy account, assigned number, call status and duration, and related transaction or device records.

Depending on risk and the available evidence, the Company may:

- restrict or suspend the account while the investigation is pending;
- deactivate account devices and prevent issuance of new sessions;
- block further number purchases;
- ask the wholesale carrier to block or terminate traffic or service;
- preserve relevant records;
- require enhanced identity or business-purpose verification;
- terminate the customer relationship; and
- report or refer the matter to the carrier, the Industry Traceback Group, the FCC, or law enforcement.

The administration system records fraud flags and administrative actions in an audit trail. Because account suspension alone may not immediately invalidate every previously issued short-lived access token, urgent cases require the reviewer also to request carrier-level blocking or termination and to verify that calling has stopped. This escalation remains in place until the Company deploys and verifies per-request active-account enforcement.

7. Traceback cooperation

The Company commits to respond fully and within 24 hours to traceback requests from the Federal Communications Commission, law enforcement, and the registered industry traceback consortium, and to cooperate in investigating and stopping illegal robocallers that use its service.

Requests should be sent to fawad@createchagency.com and may also be made by telephone at +92 315 9585665. The mailbox is the designated compliance contact. The Company will acknowledge a qualifying request, preserve responsive records, search the call-history and account records, identify the upstream or downstream provider where available, provide responsive information lawfully available to it, and take prompt steps to stop confirmed or credibly suspected illegal traffic.

CallEazy call-history records associate the customer account with the assigned originating number, destination number, direction, status, provider identifier where available, start time, end time, duration, provider, and charge information. Administrative search can correlate these records with the user's name, email, and telephone number. The Company will preserve relevant records when a complaint or traceback request is received and will disclose records subject to applicable law.

8. Wholesale-provider cooperation

The Company maintains operational account information for the wholesale providers used to supply numbers or route traffic. Its currently integrated SIP voice provider is IDT Express. Other carriers are not treated as active production providers until their service and controls are integrated and approved. The Company will cooperate with its carriers on caller-ID validation, traceback, investigation, traffic

blocking, and account termination, and will provide its Robocall Mitigation Database identifier when required.

Before enabling a new carrier for production traffic, the Company will document the carrier’s support and abuse contacts, caller-ID rules, traceback procedure, and applicable STIR/SHAKEN role.

9. Training, testing, and program review

Personnel with administrative access to fraud, account, and call-history tools must use those tools only for authorized support, security, compliance, and investigation purposes. Material mitigation actions should state the reason and be retained in the administrative audit record.

The program owner will periodically confirm that the designated contact remains reachable, the call history can be searched using the identifiers normally supplied in a traceback request, suspension and carrier-escalation procedures work, and carrier contacts are current. Identified gaps will be documented, prioritized according to risk, and corrected.

10. Certification scope

This document describes the Company’s robocall mitigation program as adopted on the effective date. It does not claim that CallEasy itself cryptographically signs calls, that every customer has completed government-identity verification, or that anomaly indicators automatically block calls. The Company will not represent an upstream carrier’s STIR/SHAKEN implementation as its own.

The Company’s no-implementation certification uses the lack-of-network-control explanation contemplated by 47 CFR § 64.6305(d)(2)(i), not a claim that foreign-provider status alone is an exemption under 47 CFR § 64.6306.

Approved for CREATECH INFORMATION TECHNOLOGIES (PRIVATE) LIMITED:

Fawad Anwar, CEO
Document/adoption date: October 6, 2026