Robocall Mitigation Program Description

This draft describes the robocall mitigation program of Upword Solutions Inc, DBA Innovatek Solutions for its Robocall Mitigation Database filing under 47 CFR § 64.6305.

1. Provider information and program overview

Upword Solutions, Inc. (FRN 0037483070, 0039071576. Upword Solutions is a voice service provider that provides hosted VoIP to small businesses in Ohio.

This document describes the specific, reasonable steps Upword Solutions has taken to avoid originating, carrying, or processing illegal robocall traffic. The program applies to all calls on the company's network, including calls it originates, carries, and terminates, and calls received from other providers.

The program rests on five commitments, each described below:

- Authenticate calls with STIR/SHAKEN wherever the company is able to do so.
- Know who its customers are before activating service and while service continues.
- Know and vet the upstream providers from which it accepts traffic.
- Monitor traffic and act promptly on suspected illegal robocalls.
- Respond to traceback requests within 24 hours and keep its RMD filing accurate.

2. Caller ID authentication (STIR/SHAKEN)

Implementation status

- Full implementation: Upword Solutions has implemented STIR/SHAKEN on the IP portions of its network. It signs calls it originates with its own SPC token and a certificate from an authorized STI-CA, and it verifies the identity headers on calls it receives.]

Attestation practice. Upword Solutions assigns attestation levels only on information it can verify. It gives A-level attestation when it has authenticated the customer and confirmed the customer's right to use the calling number, B-level when it has authenticated the customer but cannot confirm the number, and C-level for calls entering from sources it cannot authenticate

3. Know your customer

Upword Solutions does not activate voice service, assign numbers, or accept traffic from a customer until it has completed the following steps.

Identity and business verification. Collect the customer's legal name, physical address, principal contact, and website. Verify the business through [secretary of state records / credit or identity-verification vendor / government ID for individuals].

1. **Intended use.** Obtain the customer's description of its calling use case (e.g., customer service, appointment reminders, telemarketing, call center) and expected call volumes. Customers that place outbound telemarketing or high-volume automated calls are subject to enhanced review.

2. **Number authority.** Confirm the customer's right to use each calling number it will present as caller ID, through [number assignment records / porting records / letters of authorization / customer certification and spot checks].
3. **Acceptable-use agreement.** Require every customer to agree in writing that it will not originate illegal robocalls or spoofed calls, will comply with the TCPA and Telemarketing Sales Rule, and will cooperate with tracebacks. The agreement permits [Company Legal Name] to suspend or terminate service immediately for violations.
4. **Risk tiering and limits.** Assign each customer a risk tier at onboarding. [Describe limits for new or high-risk customers, e.g., call-per-second caps, daily volume caps, restricted outbound calling until review is complete.]
5. **Ongoing review.** Re-review customers [annually / when usage changes materially / on any complaint or traceback]. Review call-pattern metrics described in section 5 and update the customer's risk tier.
6. **Prohibited customers.** Do not onboard customers previously terminated by [Company Legal Name] for robocall violations, and screen new customers against [FCC RMD removal lists / FCC enforcement orders / internal block list].

Records. Upword Solutions keeps onboarding files, agreements, and number-authority evidence for at least 10 years after service ends.

4. Know your upstream provider

Upword Solutions accepts voice traffic only from providers that appear in the FCC's Robocall Mitigation Database and have a current, non-deficient filing. Before accepting traffic from a new upstream provider, and at least [annually] afterward, the company:

- Confirms the provider's RMD listing and that its robocall mitigation plan describes specific, reasonable steps.
- Obtains the provider's written commitment to cooperate with tracebacks and to prevent illegal robocalls on traffic it sends.
- Reviews the provider's business history, ownership, and regulatory or enforcement actions, using [public FCC records / vendor tools / questionnaire].
- Asks the provider to describe how it vets its own customers and upstream sources.
- Starts new providers at limited volume or restricted routes and monitors their traffic closely for 30 days.

If an upstream provider is removed from the RMD, fails to respond to tracebacks, or repeatedly sends traffic identified as illegal, Upword Solutions stops accepting its traffic, and notifies the Industry Traceback Group / the FCC, where appropriate. Contracts with upstream providers include a right to suspend traffic for these reasons.

5. Monitoring and mitigation

Upword Solutions monitors traffic on its network for patterns associated with illegal robocalls, using [describe tools, e.g., in-house CDR analysis / a named analytics vendor / a session border controller with rate controls]. Monitoring covers calls the company originates and traffic it receives from upstream providers.

Indicators reviewed.

- Very short average call duration and high rates of calls under 6 seconds
- Low answer-seizure ratios and high volumes of sequential or randomly generated dialing
- Large volumes from a single account or number block, or sudden volume spikes
- Calling numbers that are invalid, unallocated, or on Do Not Originate lists
- Many different caller IDs sent by one customer, or caller IDs the customer cannot show it is authorized to use
- Complaints, traceback requests, and consumer-complaint data tied to a customer or upstream provider

Response steps. When an indicator is triggered, Upword Solutions reviews the traffic within 3 business days. If the traffic appears to be illegal, the company [throttles or blocks the traffic / suspends the account and requires the customer or upstream provider to explain the traffic and show that the calls are lawful before restoring service. Customers that originate illegal robocalls are terminated, and repeated violations by an upstream provider lead to blocking all of its traffic.

Do Not Originate and blocking. The company blocks calls that purport to come from numbers on its Do Not Originate list and from invalid, unallocated, or unassigned numbers, [and it applies network-level blocking to calls identified in FCC-authorized blocking categories]. It never blocks calls to 911 or other emergency numbers, and it makes reasonable efforts not to block calls from public safety answering points and government emergency numbers.

6. Traceback and RMD maintenance

Traceback. [Company Legal Name] commits to respond fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. The company is registered with the [Industry Traceback Group USTelecom portal, and it maintains a monitored contact, role-based email address and phone, so that requests reach someone authorized to act on them at any hour. On receiving a request, the company identifies the source of the traffic, whether a customer or an upstream provider, and gives the requesting party the information it needs. It then takes the mitigation steps in section 5.

RMD filing. Upword Solutions has filed a certification and this program description in the Robocall Mitigation Database. It updates its filing within 10 business days of any change to the information filed, including any change to the contents of this description. It recertifies its filing annually by the FCC's deadline, which has been March 1 under the current rules.

Prior actions. [State whether the company or any of its affiliates, owners, officers, or principals has been the subject of a Commission, law enforcement, or regulatory action or investigation relating to unlawful robocalls, and give the details required in the filing. If none: "None."]

7. Governance, training, and recordkeeping

Matt Towers is the officer responsible for this program and for the accuracy of the company's RMD filing. He reviews this description at least [annually] and whenever the company's services, network, customers, or the FCC's rules change, and approves any change before it is filed.

Employees who onboard customers, operate the network, or handle traceback and complaint requests receive training on this program when they start and [annually] afterward. [Describe any additional internal controls, such as a second-person review before activating high-volume customers.]

Upword Solutions keeps records of customer vetting, upstream-provider reviews, traffic investigations, blocking and termination decisions, and traceback responses for at least 10 years.