

ROBOCALL MITIGATION PROGRAM DESCRIPTION UBIK Inc.

Date: December 16, 2025 **FCC Registration Number (FRN):** 0031450760 **Operating Company Number (OCN):** 184L **Address:** 1605 Chemin Ste-Foy, QC G1S 2P1 QUEBEC, Canada

1. Overview

UBIK Inc. ("UBIK") is a voice service provider offering VoIP services to end-users in Canada and the United States. UBIK has implemented the STIR/SHAKEN authentication framework across its network. In addition to STIR/SHAKEN implementation, UBIK maintains a robust Robocall Mitigation Program ("RMP") designed to prevent the origination of illegal robocalls, prevent spoofing, and comply with all FCC and CRTC requirements.

2. Know-Your-Customer (KYC) and Vetting

UBIK allows access to its network only after a vetting process to verify the identity of the subscriber. Our KYC protocols include:

- **Financial Verification:** We require a valid credit card for all accounts. We verify the validity of the payment method and the associated billing information before service activation. This creates a traceable financial trail for every subscriber.
- **Account Vetting:** We review customer information upon signup to ensure legitimacy. Anonymous usage of our network is not permitted.

3. Call Blocking and Do-Not-Originate (DNO) Compliance

In compliance with FCC Report and Order FCC 24-114 (effective December 15, 2025), UBIK actively blocks calls that attempt to originate from numbers on a reasonable Do-Not-Originate list.

- **Invalid Number Filtering:** UBIK utilizes custom in-house software to analyze the "From" field (Caller ID) of outbound calls. Calls attempting to originate from invalid formats (e.g., unallocated area codes, invalid NANP formats) are blocked at our network edge.
- **Upstream Enforcement:** We utilize the blocking and filtering capabilities of our upstream carrier, Bandwidth.com, to ensure that calls originating from invalid, unallocated, or "inbound-only" numbers are rejected before reaching the PSTN.
- **Redress Mechanism:** In the event a legitimate call is blocked erroneously, UBIK maintains a point of contact for blocking disputes. Subscribers or other callers may contact [\[abuse@ubikvoip.com\]](mailto:abuse@ubikvoip.com) to request an investigation.

4. Network Monitoring and Traffic Analysis

UBIK employs a multi-layered approach to monitor for and mitigate suspicious traffic patterns:

- **International Blocking:** By default, UBIK blocks international outbound calling for customer accounts. This significantly reduces the risk of high-cost fraud or international revenue share fraud (IRSF) originating from our network.
- **High-Volume Monitoring:** We collaborate closely with our upstream carrier, Bandwidth.com, to monitor traffic for signatures of illegal robocalling, such as high-volume, short-duration (HVSD) calls.
- **Alerting and Suspension:** Upon receiving an alert from our internal systems or our upstream carrier regarding suspicious traffic, UBIK investigates immediately. If illegal activity is confirmed or suspected, we take prompt action, which may include suspending the offending account and blocking the traffic source.

5. Cooperation with Industry Traceback

UBIK is fully committed to cooperating with the FCC, law enforcement, and the Industry Traceback Group (ITG). We are committed to responding fully and within 24 hours to all traceback requests to identify the source of illegal traffic and will terminate services for any customer found to be originating illegal robocalls.