

SKAIVISION ROBOCALL MITIGATION PROGRAM DESCRIPTION

Filer: SKAIVISION

Provider Type: Voice Service Provider

STIR/SHAKEN Certification Status: No STIR/SHAKEN Implementation

1. Overview of SKAIVISION's Services

SKAIVISION provides communications-enabled software and services to automotive dealership customers. SKAIVISION's services are used by dealerships to communicate with their own customers, including service customers, sales customers, and other dealership contacts. SKAIVISION uses Bandwidth as its underlying communications provider for PSTN-enabled telephone numbers and related voice-capable services.

SKAIVISION is not a facilities-based voice carrier and does not own or control the underlying PSTN/IP voice network infrastructure, switching, SBCs, numbering resources, interconnection facilities, or STIR/SHAKEN certificate infrastructure used to authenticate calls. SKAIVISION relies on Bandwidth and other upstream providers, as applicable, for underlying network connectivity, number provisioning, routing, and carrier-level controls.

SKAIVISION does not operate as a gateway provider for foreign-originated traffic entering the United States and does not operate as a non-gateway intermediate provider that merely carries or processes third-party voice traffic without originating or terminating such traffic.

2. STIR/SHAKEN Implementation Status and Applicable Exemption

SKAIVISION has selected "No STIR/SHAKEN Implementation" because SKAIVISION has not implemented the STIR/SHAKEN authentication framework on any portion of its own network.

SKAIVISION relies on the exemption in 47 CFR § 64.6304(b) for providers that are incapable of obtaining an SPC token due to Governance Authority policy, to the extent applicable. SKAIVISION does not own or control the network infrastructure necessary to directly implement STIR/SHAKEN authentication and does not independently operate the network elements required to sign outbound calls using its own STIR/SHAKEN certificate. SKAIVISION uses Bandwidth as its underlying voice service provider/carrier for PSTN-enabled telephone numbers and outbound/inbound voice routing.

Because SKAIVISION lacks control over the network infrastructure necessary to implement STIR/SHAKEN directly, SKAIVISION is currently unable to implement STIR/SHAKEN authentication on its own network. SKAIVISION will update its Robocall Mitigation Database filing if its STIR/SHAKEN implementation status, provider role, network control, or applicable exemption changes.

3. Robocall Mitigation Program

SKAIVISION maintains a robocall mitigation program designed to prevent the origination of illegal robocall traffic through its services. SKAIVISION's program includes customer vetting, use-case review, telephone number and campaign controls, opt-out/suppression procedures, logging, monitoring, upstream-provider cooperation, and traceback response procedures.

SKAIVISION's services are intended for legitimate dealership communications with customers who have an existing relationship with the dealership or who have otherwise provided appropriate authorization or consent. SKAIVISION does not knowingly support illegal robocalling, caller ID spoofing, fraudulent traffic, scam traffic, or high-risk anonymous calling campaigns.

4. Customer Vetting and Know-Your-Customer Procedures

SKAIVISION takes reasonable steps to know its customers and the use cases for which SKAIVISION-provided communications services are used. SKAIVISION's direct customers are business entities, primarily automotive dealerships or dealership groups.

Before enabling communications services, SKAIVISION reviews customer identity and business information, which may include legal business name, dealership name, business address, website, authorized contacts, and the intended communications use case. SKAIVISION also reviews whether the communications are intended for existing dealership customers, service customers, sales customers, or other authorized contacts.

SKAIVISION does not intentionally permit anonymous use of its communications platform. Customer accounts are associated with identifiable business entities and authorized users. SKAIVISION may suspend, restrict, or terminate communications access for customers or users that provide false information, use SKAIVISION services for unlawful purposes, fail to cooperate with compliance reviews, or generate traffic that appears unlawful, abusive, fraudulent, or inconsistent with the approved use case.

5. Use-Case Controls

SKAIVISION's communications use cases are limited to dealership-related customer communications. Examples may include service communications, vehicle-related customer engagement, appointment-related communications, trade-in or purchase-related communications, and follow-up communications related to the dealership-customer relationship.

SKAIVISION does not knowingly permit its platform to be used for illegal robocalling, scam campaigns, fraudulent lead generation, impersonation, unlawful spoofing, or other traffic that violates applicable law or carrier requirements.

Where applicable, SKAIVISION uses 10DLC registration, campaign review, and carrier approval processes through its upstream provider. SKAIVISION expects customer

communications to be consistent with the approved campaign/use case, applicable consent requirements, opt-out rules, and carrier messaging policies.

6. Telephone Number and Caller ID Controls

SKAIVISION uses telephone numbers provisioned through its upstream provider, Bandwidth, and associates numbers with approved customer/use-case configurations.

SKAIVISION does not knowingly allow customers to transmit false, misleading, or spoofed caller ID information. Numbers used in connection with SKAIVISION services are intended to identify a legitimate business communication path associated with SKAIVISION, the dealership customer, or the applicable campaign.

Where a telephone number is presented to an end user and inbound voice functionality is applicable, SKAIVISION's recommended operational practice is to route inbound calls to the dealership, SKAIVISION, or another authorized customer-service destination so that call recipients have a reasonable means of contacting the seller or service provider associated with the communication.

7. Opt-Out, Suppression, and Do-Not-Contact Controls

SKAIVISION maintains opt-out and suppression controls for customer communications. When an end user requests not to receive further communications, SKAIVISION logs and applies the opt-out or suppression status as applicable to prevent further communications to that end user through SKAIVISION-managed workflows.

SKAIVISION supports standard opt-out handling for SMS communications, including suppression of numbers that opt out through recognized opt-out keywords or other documented opt-out requests. SKAIVISION also communicates opt-out information to the dealership customer when appropriate so the dealership can update its own internal systems and customer contact preferences.

SKAIVISION expects dealership customers to honor customer opt-out requests and to comply with applicable federal and state calling and texting laws, including do-not-call, consent, and customer-contact requirements.

8. Monitoring, Logging, and Abuse Detection

SKAIVISION maintains logs and system records related to communications activity, including customer account information, campaign/use-case information, telephone numbers, message/call activity where applicable, timestamps, and opt-out events. These records support operational monitoring, customer support, compliance review, and traceback response.

SKAIVISION monitors for indications of improper or abusive use of its platform, which may include unusual traffic volume, unusual calling or messaging patterns, complaints, carrier notices, opt-out spikes, customer support escalations, failed delivery patterns, or other indicators of potentially non-compliant activity.

If SKAIVISION identifies suspicious, unlawful, or non-compliant activity, SKAIVISION may investigate the activity, contact the customer, restrict or suspend communications, suppress affected numbers, modify campaign settings, escalate the matter to its upstream provider, or terminate access to SKAIVISION communications services.

9. Analytics and Blocking Systems

SKAIVISION uses internal operational controls, logging, monitoring, customer/use-case controls, opt-out suppression, and upstream-provider processes to identify and mitigate potentially unlawful or abusive communications traffic.

SKAIVISION does not currently operate its own standalone STIR/SHAKEN signing infrastructure or carrier-grade voice analytics platform. SKAIVISION relies on Bandwidth

and other applicable upstream providers for underlying network-level capabilities, carrier routing, number provisioning, and any upstream network-level mitigation, analytics, blocking, or enforcement processes that apply to traffic carried on their networks.

Third-party analytics vendors used directly by SKAIVISION for voice-call analytics: None at this time.

If SKAIVISION later implements or directly contracts for a third-party analytics or blocking system for voice traffic, SKAIVISION will update this Robocall Mitigation Database filing as required.

10. Upstream Provider Procedures

SKAIVISION uses Bandwidth as its underlying communications provider. SKAIVISION cooperates with Bandwidth's requirements for number provisioning, campaign registration, compliance review, acceptable use, messaging/voice policy enforcement, and abuse mitigation.

If Bandwidth or another upstream provider notifies SKAIVISION of suspected unlawful traffic, complaint activity, traceback activity, campaign non-compliance, or other abuse indicators, SKAIVISION will investigate promptly and take appropriate corrective action. Corrective action may include customer outreach, traffic review, suppression, number or campaign changes, suspension of communications functionality, or termination of the customer's access to affected services.

11. Traceback Response Commitment

SKAIVISION commits to respond fully and within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement, and the registered Industry Traceback Group/industry traceback consortium.

SKAIVISION will cooperate with the Commission, law enforcement, the Industry Traceback Group, Bandwidth, and other relevant providers in investigating and stopping illegal robocallers that may attempt to use SKAIVISION's services. SKAIVISION will use available account records, customer information, number assignment information, logs, timestamps, and other relevant records to identify the source of traffic and support traceback investigations.

12. Investigation and Enforcement Procedures

Upon receiving a traceback request, complaint, carrier notice, or other indication of potentially unlawful traffic, SKAIVISION will review available records to identify the customer, campaign, telephone number, workflow, and user or system activity associated with the traffic.

Depending on the findings, SKAIVISION may take one or more of the following actions:

- Contact the customer for explanation and remediation;
- Require confirmation of the customer's use case, authorization, consent practices, and contact-list source;
- Suppress affected telephone numbers or end-user contacts;
- Disable or restrict the relevant workflow, campaign, user, or customer account;
- Suspend or terminate communications services;
- Escalate the matter to Bandwidth or another upstream provider;
- Preserve and provide records as appropriate in response to lawful traceback, regulatory, or law-enforcement requests.

13. Customer Obligations

SKAIVISION requires customers to use SKAIVISION services only for lawful purposes and only in connection with legitimate dealership communications. Customers are expected to comply with applicable federal and state laws and regulations governing calls, texts, consent, opt-outs, caller ID, do-not-call obligations, and consumer protection.

SKAIVISION does not knowingly permit customers to use its services for unlawful robocalls, unlawful spoofing, fraudulent traffic, scam campaigns, or communications to individuals who have opted out or otherwise should not be contacted.

14. Recordkeeping

SKAIVISION maintains relevant operational and compliance records to support its robocall mitigation program. These records may include customer account information, authorized contacts, telephone number assignments, campaign/use-case details, opt-out and suppression records, activity logs, and investigation notes.

SKAIVISION uses these records to support compliance monitoring, customer support, complaint investigation, traceback response, and cooperation with Bandwidth, the FCC, law enforcement, and the Industry Traceback Group.

15. Program Updates

SKAIVISION will periodically review and update its robocall mitigation program as its services, provider relationships, regulatory obligations, STIR/SHAKEN implementation status, or risk profile changes.

SKAIVISION will update its Robocall Mitigation Database filing within the time required by FCC rules if any information in the filing materially changes, including changes to provider role, STIR/SHAKEN implementation status, robocall mitigation measures, traceback contact information, or other required filing information.

16. Certification Statement

SKAIVISION certifies that all calls it originates through its services are subject to this robocall mitigation program. SKAIVISION has taken and will continue to take reasonable steps to avoid originating illegal robocall traffic. SKAIVISION commits to respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group/industry traceback consortium, and to cooperate with such entities in investigating and stopping illegal robocallers that may use SKAIVISION's services.