



WHITE PAPER · FOR SERVICE BUSINESSES, DEALERSHIPS, PROPERTY OPERATORS, AND PRACTICES MAKING CUSTOMER CALLS OR SENDING REMINDERS

Fixing business call labels and text delivery

Managing caller identity and messaging registration for customer communications

Authenticate the calling identity, investigate the actual label, and verify messaging registration separately from recipient permission.

PUBLISHED BY
Greg Steinig, SPARK VoIP

DATE
October 2026

RESEARCH REVIEWED THROUGH
October 4, 2026

Executive summary

A legitimate business can encounter a Spam Likely label, a blocked call, a low answer rate, or rejected texts. Those symptoms should not be treated as one failure. Call authentication, reputation analysis, caller-name display, messaging registration, and recipient permission are separate systems with different evidence and remedies.

STIR/SHAKEN carries signed calling identity information. A is full attestation, B is partial attestation, and C is gateway attestation. These categories express the signing provider's asserted knowledge of the call's origin and number use. They do not rate business quality, certify lawful purpose, or promise a favorable display. [1, 6]

The cited messaging provider requires A2P 10DLC registration for its application messaging to US recipients from local ten-digit numbers. Manual staff messages can fall within that scope. Registration and recipient permission are separate; voice authentication does not register texting. Check the purchased provider and number type. [3, 4]

Key findings

- 01 Attestation describes asserted identity knowledge; authenticated calls can still be unwanted. [1, 6]
- 02 A warning label, a blocked call, and an unanswered call require separate evidence.
- 03 Caller-name data and reputation are separate from signed call identity.
- 04 Manual business-app texts can require registration; approval does not establish recipient permission. [3, 4]
- 05 A useful support case includes the number, route, recipient carrier, time, and observed symptom.

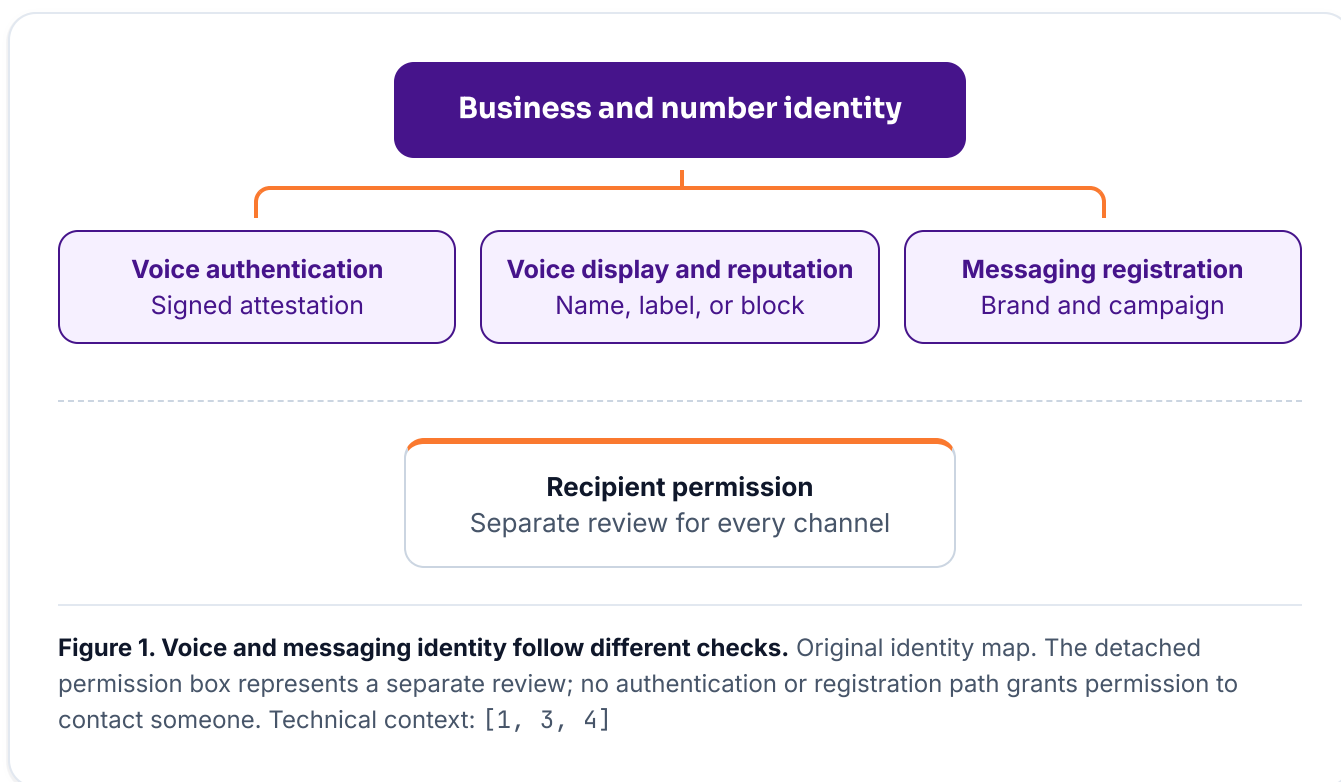
Use an evidence-based repair process for each channel, supported by stable identity and approved contact practices. This paper covers US customer communications. No observed repair outcome or carrier-wide improvement is established; test the actual results for your numbers and routes.

Separate the five identity and delivery layers

SIP means Session Initiation Protocol, the signaling protocol used to set up many IP telephone calls. STIR/SHAKEN is a caller-ID authentication framework. A2P means application-to-person messaging; 10DLC means a ten-digit long code. These labels describe technical processes, not proof of a recipient's permission.

The visible caller name can come from a directory or branded-calling service. Signed identity, reputation analysis, and device settings serve different functions. This is a diagnostic model, not a disclosure of any carrier's proprietary decision rules. There is no single global reputation score established by the cited evidence; test each relevant network and route.

Begin with the symptom. Did the call fail to reach the device, ring with a warning, display the wrong name, or simply go unanswered? For a text, was the failure a registration rejection, a carrier error, an unsupported number, or a recipient opt-out? A case described only as "our calls are spam" does not give support enough evidence to identify the layer.



Owning or managing a SIP service gives a provider useful route information, but it does not by itself establish authority to sign every call or control each receiving network's analytics. Ask which carrier originates the call, which entity signs it, and how the business's right to use the

number is verified.

03

Understand what attestation can prove

ATIS-1000074.v003 section 5.2.4 defines attestation. A and B both require responsibility for IP-network origination and an authenticated, identifiable customer relationship. A adds a verified number association; B lacks it. C applies at a gateway or when information is insufficient for A or B. [1, 6]

A
Full attestation
Authenticated customer and verified number association

B
Partial attestation
Authenticated customer; number association unverified

C
Gateway attestation
Gateway context or insufficient information for A or B

Table 1. Identity and delivery signals

Signal	What it indicates	What it does not establish
A full attestation	Authenticated customer and verified number association	Lawful purpose, wanted content, or a favorable display
B partial attestation	Authenticated customer; number association unverified	Fraud or a known cause of a warning
C gateway attestation	Gateway context or insufficient information for A or B	Verified originating customer or a business-quality score
Caller name	Name display from supported identity service	Attestation or universal handset display
10DLC registration	Approved provider brand and campaign relationship	Permission for every recipient or every message

Summarizes attestation using the ATIS standard and informative technical report; registration uses provider documentation. A category does not establish call legitimacy. [1, 3, 6]

A lower attestation alone cannot explain a warning. Separate a call that rings with a label from a call that is blocked. Current 47 CFR 64.1200(k)(8) addresses terminating-provider contacts for blocking errors and adverse authentication treatment; it does not promise universal label

removal. [2]

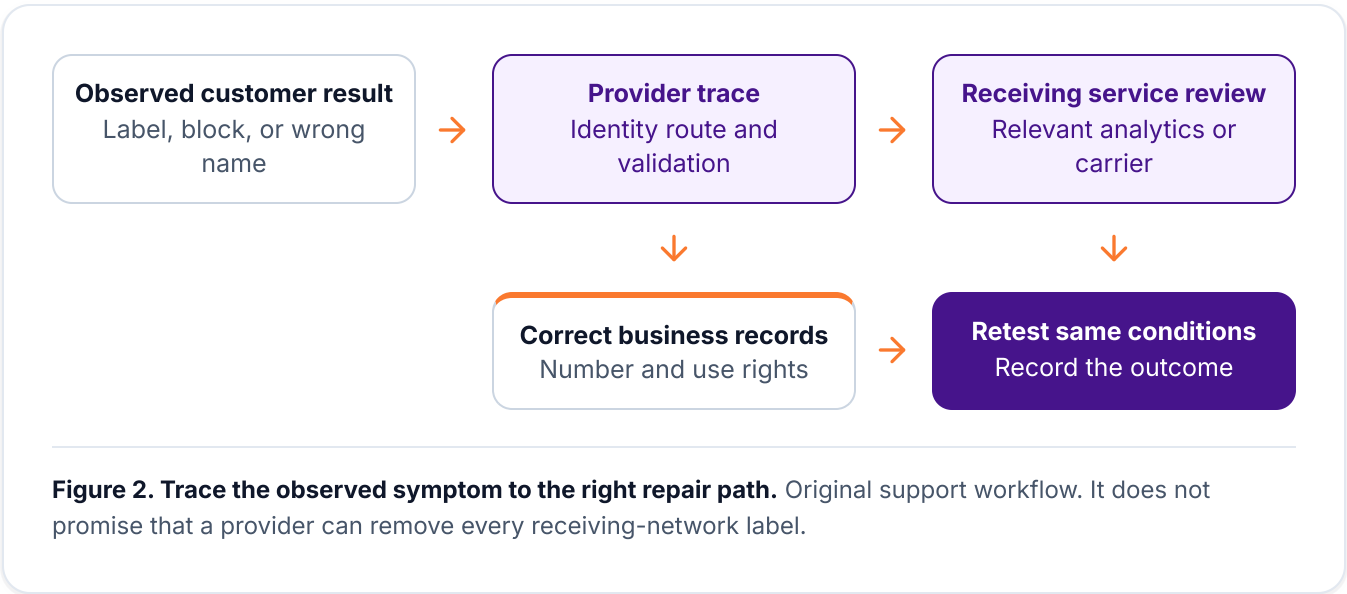
Request the attestation and signature-validation result for representative calls. The cited voice provider’s technical guide reports those as distinct evidence. A validated signature does not convert B or C to A. Check the presented number, route, forwarding behavior, and number authorization with the actual originating provider. [8]

Current 47 CFR 64.6301(a) addresses voice-provider authentication in IP networks, subject to its exceptions. Paragraph (b) permits third-party authentication under stated conditions, retaining the provider’s attestation decisions and certificate. Ask who is responsible for the proposed route; PBX ownership alone does not answer that question. [7]

04

Build a useful voice support case

Collect examples across relevant receiving networks using consenting test recipients. Record call identifiers, caller and destination numbers, timestamp and time zone, originating route and signer, recipient carrier, exact label, ring or block outcome, and handset settings. Retain screenshots and the matched provider trace. A screenshot alone cannot locate the decision in the call path.



The cited voice provider’s documentation describes a process for submitting business numbers to analytics providers. That is one provider’s product workflow, not an industry-wide guarantee or evidence of SPARK VoIP’s supplier relationships. Ask the actual carrier which supported submission and redress channels it offers. [5]

Keep numbers stable when practical and review contact behavior. Identify the business, match the customer’s context, honor preferences, and follow the approved contact policy. Do not rotate numbers to evade unwanted-contact controls. Even correctly authenticated traffic can remain unwanted. These are operating recommendations, not measured repair effects.

Track label observations, ringing, blocking, answers, and completed business outcomes separately. A changed display does not establish a revenue effect. Before crediting remediation, compare call volume, purpose, content, audience, timing, recipient availability, and route. Record changes that prevent a fair comparison.

05

Register texting without confusing it with consent

For the cited provider’s US local-number application workflow, register the brand and campaign. Toll-free numbers and short codes use separate processes. Ask the purchased provider to confirm number eligibility, campaign class, samples, fees, approval, and supported throughput. Table 3 defines the scope to check. [3]

Table 2. Message launch evidence

Record	Why it is needed	Owner
Business identity	Matches the legal sender and supported number	Business administrator
Campaign description	Matches the actual message purpose and examples	Messaging owner
Purpose-specific permission	Links recipient, sender, subject, permission date and method, and withdrawal status	Customer-facing team
Opt-out handling	Tested sender-level suppression across staff and automated sends; approved re-consent process	Platform and operations
Delivery evidence	Separates provider acceptance, reported delivery, error, and recipient observation	Carrier support and operations

Original launch control matrix. Registration, purpose-specific permission, and opt-out operation need separate evidence. It is not a complete legal checklist. [3, 4]

The cited Messaging Policy, updated April 13, 2026, permits replies to an inbound question without granting recurring-message permission. Informational messages require prior express consent; promotional messages require prior express written consent, subject to the full policy. Identify the sender and retain permission evidence. After opt-out, it allows one confirmation; subsequent messages require new express written consent. These are the cited provider's terms, not universal law or other providers' contracts. [4]

Map each campaign to its actual purpose and permission record. Keep the sender, recipient, approved subject, date and method of agreement, applicable terms, and withdrawal status. An appointment reminder and an offer need separate scope review. Counsel should assess current applicable law for the actual workflow; a CRM entry or registration approval cannot settle that analysis.

Budget campaign registration, recurring fees, message usage, and operational support. Approval timing and throughput are provider-specific. Do not advertise texting on a ported number until the receiving workflow has been accepted and tested.

SPARK VOIP TEXTING REGISTRATION

SPARK VoIP handles brand and campaign registration for texting. SMS/10DLC registration is Do not advertise texting on a ported number until the receiving workflow has been accepted and tested.

50 one time, with usage metered.

06

Identify the actual messaging workflow

A receptionist typing an individual text in a business application is still using an application. Under the cited provider's rules, low volume or manual operation does not create a local-number registration exemption. Do not generalize that classification into a universal legal definition. [3]

Table 3. Messaging scope and provider requirements to check

Workflow	Cited provider scope	Evidence for the purchased service
US local 10DLC app messaging	Brand and campaign registration	Number type, app, campaign approval, sender linkage
Manually typed app message	Same local-number scope	Staff workflow and provider classification
Toll-free or short code	Separate process from 10DLC	Applicable verification or approval, supported use
Verification-only workflow	The cited provider's Verify is a separate option	Product eligibility and implementation terms
Another provider or route	The cited provider's terms do not decide it	Current purchased-provider rules and contract

Combines bounded provider implementation facts [3] with original procurement questions. Confirm the proposed approval, entitlement, and SPARK VoIP messaging scope in your written proposal.

Keep approval and recipient permission as distinct records

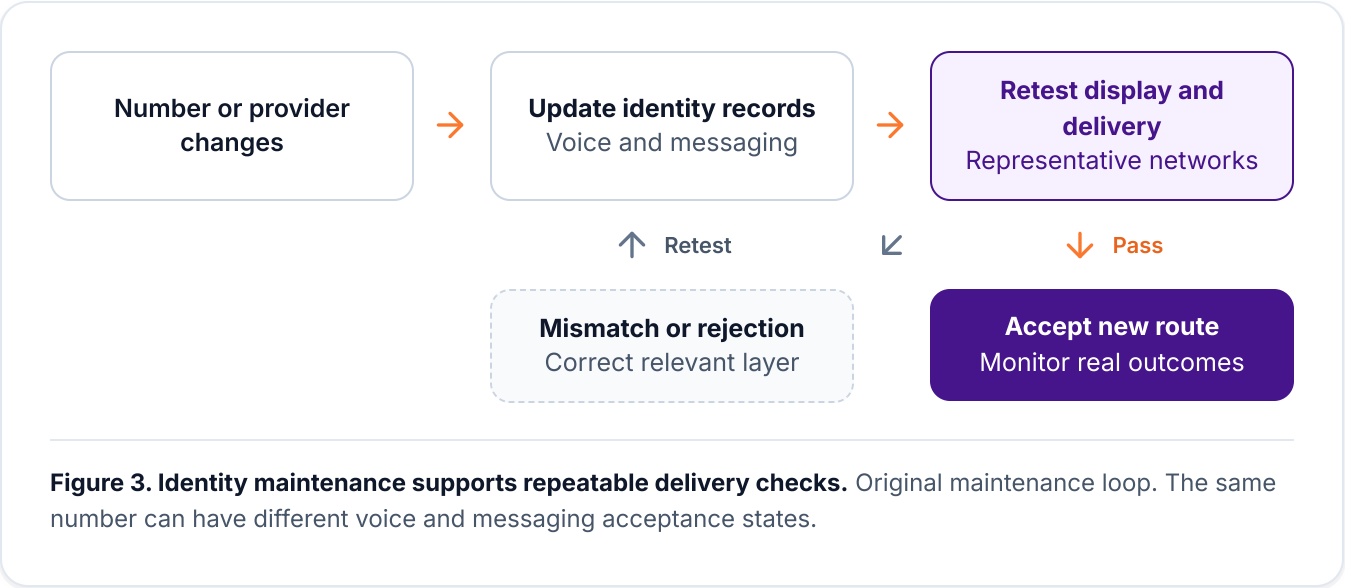
For each purpose, name the sending business, intended audience, approved content, permission evidence, suppression owner, and provider campaign. Record policy and legal review separately. A human operator needs the same approved purpose boundary as an automated sender; a staff decision to type does not expand the recipient's documented permission.

Test a permitted message and the approved opt-out path with consenting test recipients. Retain the message identifier, timestamp, sender, destination network, campaign, provider status, error code, and recipient observation. A provider acceptance status is not proof of reading; missing delivery evidence must stay unresolved.

Before a port or vendor change, obtain written confirmation of the new number-to-campaign linkage and responsibility for suppression. Keep the former service's records accessible under the approved retention process. These are operating recommendations; demonstrate the purchased service's actual behavior before launch.

Maintain identity after the repair

Number changes, ports, new departments, and vendor changes can alter the identity relationships. Maintain a record linking each number to its business owner, permitted presentation, voice route, messaging campaign, and support contact. Update it when the actual service changes.



Define the support evidence before the first incident. A small organization can use a compact case template with the fields listed in this paper. Keep any customer information limited to what the investigation needs and follow the business’s privacy policy.

For voice, verify the expected caller ID, callback route, signature result, and observed display. For messaging, verify campaign status, the sender number, representative permitted messages, opt-out behavior, and error reporting. A successful voice call does not prove any of the text tests passed.

Review the approved contact policy with new staff. Sending from the correct number is only part of an acceptable customer interaction. The business should monitor whether people recognize the sender and whether the contact frequency and purpose match their expectations.

Measure repair by network and route

Define the affected symptom and the comparison window before making a change. For each relevant recipient carrier, test each originating route the business will use, including failover or forwarding when applicable. Select networks from the actual customer footprint; record sample size and test selection. Convenience handsets are not a representative national sample.

Table 4. Carrier and route before and after record

Recipient carrier and route	Before correction	After correction	Change and evidence
Carrier 1 / route A	Test in pilot	Test in pilot	Record the actual change and paired call IDs
Carrier 1 / route B	Test in pilot	Test in pilot	Record the actual change and paired call IDs
Carrier 2 / route A	Test in pilot	Test in pilot	Record the actual change and paired call IDs
Carrier 2 / route B	Test in pilot	Test in pilot	Record the actual change and paired call IDs

Original blank test template. Carrier and route labels are placeholders, not identified networks or observations. Add rows for the actual footprint. Enter exact label and name, ring or block outcome, signature validation, and attestation in each comparison cell.

Retain reproducible evidence

Match each observation to caller and destination numbers, call ID, timestamp and time zone, originating carrier and route, signer, recipient carrier, handset, software, and blocking-app settings. Record whether the number was saved as a contact. Attach display evidence, signaling or provider trace, rejection details, and the escalation case. Missing fields remain unknown.

Change one variable at a time where feasible. Log provisioning, attestation handling, analytics submissions, caller-name updates, and contact-practice changes separately. Repeat comparable cases and state the elapsed interval. When multiple changes occur together, report the combined result without attributing the effect to one intervention.

Interpret improvement within the tested scope

Report counts and denominators for warning labels, ringing, blocking, and answers by carrier and route; retain indeterminate outcomes separately. For business answer rates, compare volume, purpose, content, audience, timing, availability, and route before assigning credit. A before-and-after difference is descriptive evidence, not proof of causation or universal clearance. No measured result is reported here.

09

Route the complaint by its actual symptom

Use Table 4 to test each relevant receiving network against each originating route. Keep carrier outcomes separate. Record the provider’s case number, requested evidence, next review date, and accountable owner. A clean display on one handset cannot clear every network or establish later delivery.

Table 5. Delivery symptoms and investigation paths

Observed symptom	First evidence to collect	Repair owner to identify
Call does not ring	Timestamp, caller and destination numbers, carrier error or trace	Originating and receiving carriers
Call rings with warning	Screenshot, receiving network, signature and attestation results	Carrier and relevant analytics service
Wrong caller name	Number, device, network, displayed name	Caller-name or branded-calling provider
Low answer rate without label	Calling period, audience, route, completed customer outcomes	Business operations
Text rejected	Message ID, error code, sender number, campaign status	Messaging provider
Recipient opted out	Consent and suppression records for the actual message type	Business messaging owner

Original diagnostic matrix. Identify the accountable owner and attach route-specific evidence before closing the case.

Retest comparable conditions after the documented correction. Keep display improvement separate from ringing, blocking, answers, and completed business outcomes. The matrix is original diagnostic guidance supported by the distinctions in [1-8]; it does not establish control over receiving-network decisions or a measured repair effect.

10

Buy visibility and a repair process

ILLUSTRATIVE SCENARIO

A hypothetical appointment reminder failure

A hypothetical practice sees its calls ring with a warning on one mobile network and its texts rejected after a number port. The call issue needs a trace and receiving-network reputation review. The text issue needs the number-to-campaign relationship checked. Registering the text campaign does not repair the voice label, and a voice authentication correction does not establish permission to message the patient.

The technical standards support separate authentication and attestation checks; current FCC rules supply bounded blocking redress duties. Provider guides describe distinct voice and messaging workflows. These sources support a symptom-based investigation, not a finding that the hypothetical repair succeeded. No test result is assumed. [1-3, 8]

Provider evaluation

Ask who decides attestation, whose certificate signs calls, what validation evidence is available, and how incorrect treatment is escalated. For texting, confirm the application, number type, registration class, purpose, and suppression process. Request route-specific demonstrations and written responsibilities. Universal clean-display or delivery promises require evidence the cited sources do not supply.

Branded calling and richer messaging are candidates for testing recipient recognition on supported networks and devices. Test coverage and benefit for your customer footprint. Compare the proposed feature against the existing route using the same outcome definitions; retain the identity, permission, and exception-handling controls.

Evaluate the correction process

Ask SPARK VoIP to trace a sample call on your numbers and show its attestation and signature result before and after any fix.

The purchase should specify responsibilities, evidence access, and unresolved gaps in writing.

References

Numbered sources support bounded factual claims. Original recommendations and models are identified. Sources were checked October 4, 2026. The eCFR displayed Title 47 current through October 1, 2026; it is authoritative but unofficial. Editions and sections are stated where established.

- [1] ATIS and SIP Forum. ATIS-1000074.v003, approved August 16, 2022. Signature-based Handling of Asserted information using toKENs (SHAKEN). Section 5.2.4, printed pages 12–13: attestation definitions. Standard text reviewed, not merely a catalog listing.
[Read source](#)
- [2] FCC rules via eCFR. 47 CFR 64.1200(k)(8)–(9) and (r). Blocking and authentication-treatment complaint contacts, analytics-blocking response codes, and text-blocking contacts. Current text reviewed; no universal label-removal promise.
[Read source](#)
- [3] Provider documentation. Programmable Messaging and A2P 10DLC. Local-number application scope, registration, and separate number-type routes. These implementation requirements are provider-specific.
[Read source](#)
- [4] Provider documentation. Messaging Policy, last updated April 13, 2026. Conversational, informational, and promotional permission; sender identity and opt-out requirements. Read the full policy and applicable terms for the actual use.
[Read source](#)
- [5] Provider documentation. Increase Call Answer Rates with Voice Integrity. Number submission to US analytics engines. Product documentation establishes a submission workflow, not independently measured delivery or universal remediation success.
[Read source](#)
- [6] ATIS. ATIS-1000088, A Framework for SHAKEN Attestation and Origination Identifier. Sections 1.2, 5.2.4, and 5.4.1–5.4.3. Informative technical report on customer authentication, number authorization, and gateway handling; not an independent legal duty.
[Read source](#)
- [7] FCC rules via eCFR. 47 CFR 64.6301(a)–(b). Voice-provider authentication obligations, referenced exceptions, and third-party arrangements. The provider retains attestation decisions and uses its certificate under the stated conditions.
[Read source](#)
- [8] Provider documentation. Trusted Calling with SHAKEN STIR. Attestation and signature-validation fields, plus provider-specific forwarding behavior. Implementation example; no SPARK VoIP supplier relationship established.
[Read source](#)

Source interpretation

The ATIS catalog identifies available standards; the actual standard and technical report were read for the cited sections. The normative definition and informative guidance have different roles. Neither document reveals a terminating carrier's complete labeling model or proves the buyer's implementation.

The cited provider documentation is primary evidence for its products and policy. Commercial claims about better answer rates or label prevention are not adopted as measured outcomes. Other providers’ terms, carrier decisions, and buyer performance need direct evidence.

FCC references support the particular provider duties described. They do not settle every telemarketing, privacy, or permission question. Review current applicable primary law and controlling decisions for the actual message purpose, technology, recipient, and jurisdiction before approving the contact process.

Methodology and research limits

The analysis separates attestation standards, FCC provider duties, provider implementation rules, recipient permission, and observed delivery. ATIS-1000074.v003 supplies normative definitions; ATIS-1000088 provides informative implementation guidance. FCC provisions supply bounded provider duties. The cited provider examples describe its products and do not establish a SPARK VoIP supplier relationship. Diagrams, matrices, and the incident example are original models; the incident is hypothetical.

Proprietary labeling decisions are not fully disclosed by these sources. Obtain route-specific evidence of carrier analytics, signing arrangements, traces, message deliveries, campaign approvals, and repair effects. No buyer tests were performed. The paper gives no fixed approval time, universal delivery assurance, or causal improvement estimate. Provider policy is distinct from law; qualified review must determine the actual legal requirements.

Evidence gaps

Obtain the originating provider and signer, route-specific attestation and validation, number presentation rights, representative receiving-network evidence, sender application and number type, campaign status, purpose-specific permission, suppression results, and error logs. Fill the proposed test matrix with real records. Confirm missing facts through written evidence and testing, rather than infer them from an approved registration or one successful call.

Figures and tables

Figure 1	Voice and messaging identity follow different checks
Table 1	Identity and delivery signals
Figure 2	Trace the observed symptom to the right repair path
Table 2	Message launch evidence
Table 3	Messaging scope and provider requirements to check
Figure 3	Identity maintenance supports repeatable delivery checks
Table 4	Carrier and route before and after record
Table 5	Delivery symptoms and investigation paths

Publication context

Assess SPARK VoIP's proposed hosted VoIP offering against the required workflows. This educational paper establishes no customer contract, legal opinion, certification, or guaranteed result. Confirm service scope, carrier relationships, support, integrations, and regulated workflows in writing for the proposed deployment.



Talk to SPARK VoIP

SALES

(888) 223-1094

SUPPORT

(918) 608-8888

WEB

sparkvoip.net

Emergency support is available 24/7.