Auto Attendant

AUTO ATTENDANT / RESEARCH & PRACTICAL GUIDANCE

Why Your Business Number Shows as Spam Likely

> Get a business phone number with a simple auto attendant menu from Auto Attendant. A caller picks who they need and the call rings that person's own mobile, so nobody on your team has to publish a personal number.

Published by Auto Attendant · 2026-09-22 · business number shows spam likely · spam likely · caller id reputation · cnam · stir shaken · free caller registry · call labeling · phone number spoofing · business phone number

Original article: https://autoattendant.io/articles/business-number-shows-spam-likely

In this article

1. Executive Summary
2. Introduction and Background
3. Quick Diagnostic: Identify the Symptom
4. The Four Systems Behind What Recipients See
5. A Step-by-Step Evidence Collection Process
6. Free Registration and Redress Routes
7. Data Analysis and Evidence
8. Prevention, Spoofing, and International Boundaries
9. Implications and Future Directions
10. Frequently Asked Questions (FAQs)
11. Conclusion

Executive Summary

A legitimate US business number can show **Spam Likely**, **Scam Likely**, **Spam Risk**, an incorrect name, or no name at all because several independent systems contribute to the recipient's screen. The fastest diagnosis begins with the exact symptom and the receiving network. Caller Name, usually called **CNAM**, supplies a name on many traditional US caller ID displays. **Secure Telephone Identity Revisited and Signature-based Handling of Asserted information using toKENs (STIR/SHAKEN)** authenticates calling-number information in Internet Protocol call signaling. A separate analytics system evaluates reputation and decides whether to warn, block, or allow a call. The Internet Engineering Task Force standard explicitly says identity verification “does not cover the display-name,” while the Federal Communications Commission says receiving providers may use authentication information to decide how to handle a call (datatracker.ietf.org) (docs.fcc.gov). An A attestation is therefore not a promise that a call will avoid a spam label.

The practical fix is to **test before registering**. Place controlled calls to consenting recipients on AT&T, T-Mobile, Verizon, and any important business destination. Record date, time, number dialed from, receiving carrier, handset, operating system or call-screening app, exact display text, whether the call rang, and a screenshot reference. A label seen on only one network points toward that network or its analytics partner; a wrong name without a warning points toward CNAM; a broad problem across networks justifies asking the originating provider to inspect number authorization, routing, and attestation. Hiya describes spam labeling as dynamic for each call, while AT&T says customer complaints and feedback contribute to Spam Risk categorization (connect-support.hiya.com) (att.com).

Use **free, first-party redress** before paying a reputation vendor. Start with the phone provider, particularly if authentication appears wrong. Eligible businesses calling on their own behalf can then use Free Caller Registry, which distributes information to First Orion, Hiya, and Transaction Network Services and states that registration is free through a centralized process (freecallerregistry.com). Its own disclaimer is decisive: **registration does not guarantee redress**, and the submitted data is not used to deliver CNAM (freecallerregistry.com) (freecallerregistry.com). If a label persists, use the named carrier or analytics-provider review route with the test log attached.

The scale explains why automated screening exists but does not prove any one business number is problematic. The Federal Trade Commission received **more than 2.6 million** Do Not Call complaints in fiscal year 2025, and explicitly cautions that the data are unverified consumer complaints (search.ftc.gov) (search.ftc.gov). The correct conclusion is procedural: isolate the responsible layer, preserve evidence, submit through the matching route, and treat any paid “guarantee” of label removal skeptically.

Introduction and Background

“Why does my business number show as spam likely?” sounds like one question, but the recipient may be seeing one of four different failures: a wrong caller name, a reputation warning, a blocked or silenced call, or a call placed by someone spoofing the business's number. Each symptom has a different data owner and a different remedy. Changing CNAM will not necessarily alter an analytics label. Registering with an analytics provider will not repair a routing or attestation problem. Filing a spoofing complaint will not update the business name shown on a landline.

This report is limited to the **United States** as of September 22, 2026. US calling-name practices, Federal Communications Commission rules, carrier analytics, and redress portals are not universal. Within the US, the terminating provider often retrieves a name using the calling-party number, while the terminating carrier is responsible for providing the Caller ID Name shown to its subscriber (docs.fcc.gov) (bandwidth.com). That division alone explains why the originating provider's records can be correct while one recipient still sees stale or different information.

The FCC required originating and terminating providers, subject to exceptions, to implement STIR/SHAKEN in the Internet Protocol portions of their networks by **June 30, 2021**; gateway providers had a separate **June 30, 2023** milestone for certain calls carrying US caller ID numbers (docs.fcc.gov) (docs.fcc.gov). These dates do not create a national “not spam” certificate. They establish an authentication framework whose signals can be combined with other information.

For a small-business owner, the decision is therefore not which reputation product to buy first. It is which system is probably wrong, who controls that system, and what evidence will make a review actionable.

Quick Diagnostic: Identify the Symptom

Begin with the recipient's exact words. “Your name looked wrong” is not equivalent to “my phone warned me about spam.” Ask for a screenshot when the recipient consents, because the label, color, icon, and call-screening app matter. Verizon notes that another app or service on a device may block a number independently of the carrier's Call Filter treatment (verizon.com).

Table 1 maps the visible symptom to the most likely system, a discriminating test, and the first owner to contact.

Observed symptom	Most likely system	Best first test	Responsible party to try first	First redress action
Wrong, old, or blank business name, but no warning	CNAM or device contact data	Call a traditional landline and two mobile networks; compare the displayed name	Originating phone provider for CNAM submission, then the receiving carrier if only one network differs	Ask what CNAM value was submitted and when; allow for database propagation
“Spam Likely,” “Scam Likely,” or “Spam Risk”	Receiving-network analytics or a screening app	Repeat the same low-volume test across AT&T, T-Mobile, and Verizon	The network or analytics provider showing the label	Register if eligible, then submit a label review with dates, times, screenshots, and affected numbers
Call is blocked, silenced, or sent directly to voicemail	Carrier blocking, device settings, or third-party app	Disable only the consenting test device's screening app and repeat once	Receiving carrier or app provider	Use its blocking or mislabeling feedback route; do not infer the cause from a missed call alone
Label appears broadly and provider logs show low or missing attestation	Originating-provider authorization, call path, or signing	Ask the provider for attestation and routing evidence for a specific call	Originating phone provider	Open a technical ticket with calling number, destination, date, time, time zone, and call identifier
People report calls that the business never placed	Number spoofing	Compare reports with provider call detail records	Originating provider and FCC complaint channel	Secure the account, preserve examples, and report the business's own number as spoofed

The table is a triage tool, not a verdict. A single recipient can have an outdated saved contact, a third-party screening app, or a carrier-specific label. Conversely, a broad pattern can involve both reputation and authentication. The useful outcome of the first round is a narrower question, such as “T-Mobile recipients see Scam Likely, but AT&T and Verizon recipients see the business name,” rather than “the number is broken.”

Three quick checks prevent common false starts:

- **Confirm the originating number.** Make sure staff are actually presenting the published business number, not a personal mobile, branch number, or temporary campaign number.
- **Separate label from name.** Ask whether the screen showed a business name, a warning, both, or neither. T-Mobile describes Scam Likely as a warning label for an incoming call it identifies as likely scam traffic (t-mobile.com).
- **Check for a local contact override.** A saved contact name can conceal the network-supplied display, so test with a consenting recipient who has not saved the number.

The Four Systems Behind What Recipients See

CNAM is caller-name data, not a trust certificate

CNAM is the caller-name information retrieved for a telephone number in the traditional US model. It is separate from the number itself and separate from a spam label. Multiple databases participate rather than one universal, instantly synchronized store. Telnyx describes “several CNAM databases” holding US-number records and says its own updates can take up to **72 hours** (support.telnyx.com) (support.telnyx.com). That provider-specific timing is an operational example, not a universal propagation guarantee.

A correct CNAM submission can solve a wrong or blank name on networks that consult the updated source. It cannot demonstrate that recipients welcome the calls, and it does not remove analytics history. Twilio similarly describes CNAM registration as displaying a business name on outbound calls to US landlines, a narrower claim than universal mobile display (twilio.com).

Branded calling adds presentation features

Branded calling is a richer presentation layer that may add a verified name, logo, and call reason. TransUnion describes it as showing “name, number, logo and call reason” beyond basic caller ID (transunion.com). Support varies by carrier, device, and service. Telnyx explicitly warns that approval does not guarantee display on every receiving carrier or device (support.telnyx.com).

Branded calling can improve identification where supported, but it is not the same as CNAM and not a universal reputation reset. A business should evaluate it as a presentation service only after correcting basic identity, authorization, and calling-practice problems.

STIR/SHAKEN authenticates calling-number information

STIR defines a signature and transport mechanism, while SHAKEN supplies the service-provider implementation profile. ATIS says the system uses **three attestation levels: Full, Partial, and Gateway** (atis.org). In common shorthand:

- **A, Full attestation.** The signing provider knows the customer, knows the call origin, and has verified the customer's association with the calling number. The STI Governance Authority description includes a “verified association with the telephone number used for the call” (sti-ga.atis.org).
- **B, Partial attestation.** The provider knows the customer and call source but has not verified the customer's association with that calling number (sti-ga.atis.org).
- **C, Gateway attestation.** The signing provider has no relationship with the call initiator and is identifying its gateway role (sti-ga.atis.org).

The attestation letter is evidence about the signing provider's knowledge, not a quality grade for the conversation. The FCC describes an Identity header traveling with the call, while the IETF treats identity verification as input to an authorization process outside the standard's scope (docs.fcc.gov) (datatracker.ietf.org). The standard also leaves forwarding or blocking subject to local policy (datatracker.ietf.org).

Reputation analytics decide warnings dynamically

Analytics providers combine signals to estimate whether a call resembles wanted, unwanted, nuisance, or suspicious traffic. The full scoring models are proprietary, so an outside article cannot responsibly assign a deterministic cause to a label. Public first-party descriptions do reveal some inputs. Hiya cites calling behavior and recipient engagement with past calls; Google says user spam reports inform its determinations; AT&T identifies customer complaints and feedback (connect-support.hiya.com) (support.google.com) (att.com).

Table 2 separates the four concepts that are most often blurred together.

Layer	What it answers	Typical output	What it does not prove	Primary correction owner
CNAM	What caller name is associated with this number in a lookup source?	Short business or personal name	That the caller is authorized, trusted, or wanted	Originating provider and relevant CNAM data source
Branded calling	What enhanced identity should a supported device render?	Name, logo, and call reason	Universal display or removal of every warning	Branded-calling provider and participating receiving network
STIR/SHAKEN	What does the signing provider know about the caller and number?	Verified Identity header and attestation	The display name, purpose of the call, or absence of spam risk	Originating provider and call-path providers
Reputation analytics	How should this particular call be treated using available signals?	Warning, category, blocking decision, or normal delivery	A permanent fact about the number or a regulator's finding	Receiving carrier, analytics partner, or device app

The comparison shows why “Does CNAM prevent Spam Likely?” and “Does STIR/SHAKEN stop spam calls?” both require the same short answer: **no**. Each can improve one input or layer, but neither controls the entire recipient experience. ATIS itself describes limited or no mitigation where calls originate or terminate on the traditional public switched telephone network (atis.org).

A Step-by-Step Evidence Collection Process

1. Freeze variables for a controlled test

Use one business number, one staff caller, and a short interval. Call only consenting test recipients. Do not create an artificial high-volume campaign. Include at least one destination on each major receiving network relevant to the business and, if customers use them, one Android phone with Google Phone and one device with a separate screening app.

Record the following for each call:

- **Origin details:** business number presented, staff endpoint, originating provider, and any campaign or branch identifier.
- **Destination details:** called number, receiving carrier, handset model, operating system, and screening app.

- **Time details:** date, local time, time zone, and provider call identifier when available.
- **Observed result:** exact name, exact warning text, whether it rang, whether it was blocked, and whether voicemail was offered.
- **Evidence reference:** screenshot filename or recipient statement, with sensitive numbers redacted when shared.
- **Consent and context:** confirmation that the recipient expected the test and whether the number was already saved as a contact.

Hiya's testing guidance says to record exactly what caller ID information appears, and USTelecom's redress guidance says an affected request may need the calling numbers plus dates and times (blog.hiya.com) (ustelecom.org).

2. Interpret the pattern, not one screenshot

A label limited to one carrier suggests a carrier or analytics review. A label limited to one handset suggests an app or device setting. A wrong name on landlines but no mobile warning suggests CNAM. A broad label across carriers, especially with unexpected attestation, merits an originating-provider review. Provider call logs can expose the attestation set by the originating service provider, where the provider makes that field available (bandwidth.com).

Do not treat a successful answer as proof that no label appeared. The called person may answer from a smartwatch, car interface, desk phone, or notification that renders less information than the handset's call screen.

3. Open one provider ticket with reproducible evidence

Ask the originating provider to confirm:

- **Number authorization:** the account is authorized to present the affected number.
- **Attestation:** the level applied to representative calls and why.
- **Call path:** whether the Identity header survived the route to the destination.
- **CNAM:** the submitted value, target database or process, and submission date.
- **Traceability:** the exact call identifiers needed for escalation.

Verizon's feedback page explicitly tells callers to contact the originating provider when caller ID authentication information appears incorrect (voicespamfeedback.com). This is the right first route for technical authentication evidence because a registry cannot re-sign a call.

4. Re-test after each material change

Use the same destinations and log format after the provider correction, CNAM update, registry submission, or analytics review. Label outcomes can be dynamic, so compare several controlled observations rather than declaring success after one clean call. Preserve the before-and-after dates. Do not increase calling volume

simply to “test the score.”

Free Registration and Redress Routes

Start with the route that owns the suspected layer

For an eligible business calling on its own behalf, Free Caller Registry is a practical centralized starting point. Its form requires business identity and contact details, a business email verification, calling purpose, an outbound-volume range, and the telephone numbers. It permits **up to 20 numbers** individually and a file upload for more (freecallerregistry.com). The form excludes service providers, business process outsourcers, and third parties attempting to register another business through that route (freecallerregistry.com).

The centralized submission reaches **First Orion, Hiya, and Transaction Network Services (TNS)**, the analytics providers associated on current first-party pages with T-Mobile, AT&T, and Verizon respectively (freecallerregistry.com) (connect-support.hiya.com) (callreporting.t-mobile.com) (spamalerts.verizon.com). These mappings can change, which is why the table below is dated.

Table 3 is a US redress directory verified on September 22, 2026. “Free” means the cited registration or feedback path says no fee or presents a free route. It does not mean the underlying phone service is free.

Route	Use it for	Eligibility and cost	Evidence or limits	Last verified
Originating phone provider	CNAM submission, number authorization, routing, or attestation	Included in the provider relationship; support terms vary	Supply a representative call ID, destination, date, time, time zone, and screenshot	2026-09-22
autoattendant.io	Provider support for customers using its one-number, mobile-routing service; not presented as an analytics registry	**$29 per month flat** for one local or toll-free business number, up to nine menu options, and unlimited receiving people (autoattendant.io) (autoattendant.io)	The first-party page documents inbound routing to existing mobiles, not a guaranteed label-removal service	2026-09-22
Free Caller Registry	One submission to First Orion, Hiya, and TNS	Businesses calling on their own behalf; free centralized process	Registration does not guarantee redress and does not supply CNAM (freecallerregistry.com)	2026-09-22
Hiya Number Registration and Support Hub	Registration or review for labels in Hiya-supported experiences	Hiya calls registration free for businesses of any size (hiya.com)	Registration reduces risk but cannot completely prevent future labels (hiya.com)	2026-09-22
T-Mobile Call Reporting and First Orion	Incorrect T-Mobile tag or direct First Orion registration	T-Mobile points businesses to a free account for bulk uploads (callreporting.t-mobile.com)	Registered businesses can file an incorrect-tag report; include network-specific examples	2026-09-22

Route	Use it for	Eligibility and cost	Evidence or limits	Last verified
TNS feedback portal	Business number mislabeled in TNS-supported treatment	Feedback form; fee not stated	The form offers the explicit option “My business number was mislabeled as spam” and accepts up to 20 additional numbers (reportarobocall.com)	2026-09-22
Verizon voice spam feedback	Legitimate calls marked as spam on Verizon	Feedback form; fee not stated	Verizon says submission may not change future labels (voicespamfeedback.com)	2026-09-22
FCC consumer complaint	The business's own number is being spoofed, blocked, or labeled	Public complaint route; not an individual label-removal service	Select “unwanted calls/texts,” then “my own number is being spoofed” (consumercomplaints.fcc.gov)	2026-09-22

The directory establishes two boundaries. First, carrier and analytics submissions are **review requests**, not purchased immunity. First Orion says registration is not a spam-tagging guarantee, and Hiya says its registration does not create a caller name or logo (firstorion.com) (hiya.com). Second, registration and CNAM are separate workstreams. If the warning disappears but the name remains wrong, finish the CNAM correction instead of resubmitting the same reputation form.

Before paying a third party, ask four questions:

- **Ownership:** Does the seller own the carrier or analytics decision, or merely submit the same free form?
- **Promise:** Is “guaranteed removal” qualified by carrier, device, time, and future calling behavior?
- **Evidence:** Will the seller provide the actual submitted records, case identifiers, and responses?
- **Scope:** Is the service correcting CNAM, adding branded calling, monitoring reputation, or disputing a label? These are not interchangeable.

Data Analysis and Evidence

Complaint totals show scale, not guilt

The FTC's fiscal year 2025 data book reported **more than 2.6 million Do Not Call complaints** and **more than 258 million active registrations** (search.ftc.gov). The FTC also reported that unwanted-call complaints were about **48% lower than fiscal year 2021**, while more than **4.7 million** additional numbers joined the registry during fiscal year 2025 (ftc.gov) (ftc.gov).

These counts establish the size of the screening problem, but they do not validate a label on any specific number. The FTC says complaint data are unverified. The FCC separately reported approximately **100,100** unwanted or illegal voice-call complaints in 2022, **84,500** in 2023, and **51,700** through August 6, 2024

(docs.fcc.gov). Different agencies, definitions, and periods mean these values should not be added into one total.

Authentication adoption is broad but not universal

The US STI Governance Authority reported **more than 1,900 participating providers** in the STIR/SHAKEN ecosystem for 2025 and said more than **550 new providers** joined during that year (cdn.atis.org) (cdn.atis.org). For historical context, the FCC said **4,948 voice providers** had filed in the Robocall Mitigation Database by September 28, 2021, of which **1,302** attested to full implementation at that point (docs.fcc.gov) (docs.fcc.gov). The denominators and dates differ, so these are milestones, not a single adoption-rate series.

The regulatory system also requires operational traceability. Current FCC materials state that providers must respond within **24 hours** to authorized traceback requests, and 2026 FCC guidance required Robocall Mitigation Database filers to update changed information within **10 business days** (docs.fcc.gov) (docs.fcc.gov). Those provider duties support traceback and mitigation. They do not impose a fixed deadline for a small business's label appeal.

What the data support

The quantitative evidence supports four restrained conclusions:

- **Screening operates at national scale.** Millions of annual complaints create pressure for automated classification.
- **Complaint counts are not adjudications.** A number can receive reports for multiple reasons, including unwanted frequency, mistaken identity, or spoofing.
- **Authentication coverage has expanded.** Thousands of providers participate in associated frameworks and databases, but legacy paths and international gateways still complicate end-to-end signaling.
- **No public conversion rate exists for label appeals.** The reviewed primary sources publish processes and disclaimers, not a reliable percentage of legitimate-business submissions that remove a label.

That last absence matters commercially. A paid service quoting a success percentage should disclose the sample, carriers, observation window, selection criteria, repeat-label definition, and whether the outcome was independently measured.

Prevention, Spoofing, and International Boundaries

Reduce avoidable reputation ambiguity

No checklist can guarantee a clean label, but disciplined operations make identity and redress easier to evaluate:

- **Use stable numbers for stable purposes.** Avoid rotating among numbers merely to escape a label. Maintain an accurate inventory; Hiya advises keeping registered telephone numbers current (developer.hiya.com).

- **Make identity consistent.** Align the legal business name, public-facing name, website, provider account, CNAM request, and registry submission. Record any legitimate trade name.
- **Set expectations.** Use a recognizable number, call when there is a legitimate relationship or clear reason, and leave a useful voicemail when appropriate.
- **Monitor recipient feedback.** Track complaint themes, opt-out requests, unanswered-call rates, and changes by receiving network. Do not infer causation from one metric.
- **Avoid misleading presentation.** Present only numbers the business is authorized to use. A technically valid A attestation does not excuse misleading call purpose or poor recipient experience.
- **Re-test after provider or campaign changes.** A new originating provider, routing path, dialer configuration, or number assignment can change what downstream systems see.

When the business number may be spoofed

Spoofing is plausible when recipients report calls absent from the provider's call detail records, especially at times or volumes inconsistent with business activity. First secure the phone-provider account and confirm that staff, integrations, and vendors did not place the calls. Preserve the reported date, time, destination, screenshot, callback behavior, and any message content without collecting more personal data than necessary.

Then contact the originating provider and use the FCC route. The FCC directs people whose own number is spoofed, blocked, or labeled to choose the **unwanted calls/texts** issue and the **my own number is being spoofed** sub-issue (consumercomplaints.fcc.gov) (consumercomplaints.fcc.gov). The agency also says it does not resolve individual unwanted-call complaints, so this report complements, rather than replaces, provider and analytics redress (consumercomplaints.fcc.gov).

Do not export US remedies globally

This article's CNAM and carrier-directory advice is US-specific. Canada requires authentication and verification of caller identification for Internet Protocol calls but cautions that not all received calls will be authenticated (crtc.gc.ca) (crtc.gc.ca). Ofcom said the United Kingdom would not proceed with Calling Line Identification authentication at that time, instead applying other network measures (ofcom.org.uk). The International Telecommunication Union likewise warns that calling-number authentication is not a global solution against fraud or spoofing (itu.int). Businesses outside the US should use their national regulator, carrier, and local analytics-provider processes.

Implications and Future Directions

The operational implication is that caller identity has become a chain of evidence, not a single database field. A business may need a correct provider account, authorized use of the number, usable STIR/SHAKEN signaling, consistent CNAM, accurate registration data, and calling behavior that recipients recognize. Because different organizations control those layers, remediation should be managed like a small incident record: owner, symptom, tested destinations, submitted evidence, case number, response, and re-test date.

For providers, clearer support records would reduce misdirected appeals. Useful records include the applied attestation, CNAM submission date and value, representative call identifiers, and the analytics route relevant to each receiving network. USTelecom maintains a directory of provider and analytics-provider redress mechanisms, but its published response targets are described as best practices rather than guarantees (ustelecom.org) (ustelecom.org).

For small businesses choosing a phone-number service, support capability deserves as much attention as headline price. **autoattendant.io** documents one local or toll-free number, inbound menu routing to existing mobiles, no per-user charge, and a flat **$29 monthly** price (autoattendant.io) (autoattendant.io). Those facts make it a direct business-number option, but its public page does not claim control over carrier spam labels. The general buying question should be whether any provider can show the number's authorization, calling-name submission, and call-level signaling when a downstream label appears.

The most useful industry improvement would be a portable, privacy-conscious receipt for each layer: who attested the number, which identity record was consulted, which analytics system made the treatment decision, and where the caller can dispute it. Until that exists, a cross-network test log is the business owner's best substitute.

Frequently Asked Questions (FAQs)

Why is my business phone number marked as spam?

The most likely categories are reputation analytics reacting to complaint or engagement signals, carrier-specific treatment, a third-party screening app, inconsistent number identity, unexpected calling patterns, weak or missing authentication, or spoofed calls using the number. A screenshot and cross-carrier test are needed to distinguish them. A label is not the same thing as CNAM.

How can a business remove Spam Likely from its number?

There is no universal removal switch. First collect controlled examples across receiving networks. Ask the originating provider to inspect authorization, routing, attestation, and CNAM. Then register through Free Caller Registry if eligible and submit a review directly to the carrier or analytics provider still showing the label. Re-test using the same destinations. Registration is evidence for review, not a guarantee.

How can a business fix caller ID reputation?

Fix the inputs that can be verified: use an authorized and stable number, keep the business and telephone-number inventory accurate, document respectful calling practices, respond to recipient feedback, and correct CNAM or attestation problems through the originating provider. If a network-specific warning remains, send the cross-carrier test log to that carrier or analytics provider. Reputation is dynamic, so continue monitoring instead of treating one clean test as permanent clearance.

What is CNAM caller ID?

CNAM is the caller-name data associated with a telephone number in common US caller ID workflows. A terminating provider can use the calling-party number to retrieve a name. Because databases and receiving services differ, recipients may see stale, abbreviated, or inconsistent names.

Does CNAM prevent Spam Likely labels?

No. CNAM can improve the displayed name, but analytics systems separately decide whether to warn or block. Free Caller Registry explicitly says its registration data is not used to deliver Caller ID Name, illustrating the separation between name data and reputation review.

What does STIR/SHAKEN do?

It carries signed information that lets providers verify what the originating provider knows about the caller and the right to use the calling number. Full, Partial, and Gateway attestations express different levels of knowledge. The framework does not authenticate the display name and does not itself decide that a call is wanted.

Does STIR/SHAKEN stop spam calls?

No. It makes caller-number spoofing harder in supported call paths and gives receiving providers an authentication signal. Receiving networks still apply local policy and analytics. Legacy and cross-border paths can also limit end-to-end authentication.

How should a business register its number with carriers?

An eligible US business calling on its own behalf can start with Free Caller Registry, which distributes information to First Orion, Hiya, and TNS. Current carrier-specific routes include T-Mobile Call Reporting with First Orion, Hiya registration and review, TNS's feedback portal, and Verizon's voice spam feedback form. Use direct, free routes first and keep every case identifier.

How long does caller reputation correction take?

The primary sources reviewed here do not establish one binding timeline. CNAM propagation, provider investigation, registry processing, analytics review, and receiving-device refresh are different processes. USTelecom publishes voluntary response targets but labels them best practices, not guarantees. Any seller promising a fixed result across every carrier should disclose the exact scope and evidence.

Conclusion

A business number usually shows as **Spam Likely** because the receiving carrier, its analytics partner, or a device app classified a particular call using reputation signals. A wrong business name is more likely a CNAM problem. A low or unexpected attestation is an originating-provider or call-path question. Reports of calls absent from business records point toward spoofing. These systems can overlap, but they should not be collapsed into one diagnosis.

The reliable sequence is simple: document the exact symptom, test across consenting recipients on different networks, ask the originating provider for CNAM and authentication evidence, use the appropriate free registration or review route, and repeat the same tests. Preserve dates, times, destinations, screenshots, call identifiers, submissions, and responses. This creates an evidence trail that a provider or analytics reviewer can act on.

CNAM does not guarantee a clean reputation label. An A attestation does not mean “not spam.” Free registration does not guarantee redress. Branded calling does not render on every device. Those limitations are not reasons to abandon remediation; they are reasons to send each problem to the organization that controls the affected layer.

For US small businesses, the practical goal is not a permanent promise that no warning can ever return. It is a defensible, repeatable process that keeps identity records accurate, detects network-specific changes early, distinguishes spoofing from genuine outbound activity, and avoids paying for a guarantee that no intermediary can honestly make.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://datatracker.ietf.org/doc/rfc8224/
2. https://docs.fcc.gov/public/attachments/FCC-23-37A1.pdf
3. https://connect-support.hiya.com/hc/en-us/articles/54311390207891-Caller-reputation-and-spam-label-help
4. https://www.att.com/legal/terms.activeArmorMobileSecurity
5. https://www.freecallerregistry.com/fcr/public/html/home.html?t=1733790392782
6. https://freecallerregistry.com/fcr/
7. https://search.ftc.gov/reports/national-do-not-call-registry-data-book-fiscal-year-2025
8. https://docs.fcc.gov/public/attachments/DA-11-1089A1.pdf
9. https://www.bandwidth.com/glossary/caller-name-cnam/
10. https://www.verizon.com/support/call-filter-faqs/
11. https://www.t-mobile.com/benefits/scam-shield
12. https://support.telnyx.com/en/articles/1130720-caller-id-outbound-vs-cnam
13. https://www.twilio.com/docs/trust-hub/registrations/cnam
14. https://www.transunion.com/faq/how-does-branded-calling-work
15. https://support.telnyx.com/en/articles/16296358-branded-calling-display-requirements
16. https://atis.org/robocalling-and-caller-id-spoofing-detect-mitigate-and-deter/
17. https://sti-ga.atis.org/wp-content/uploads/2024/01/STI-GA-Webinar-Part-3-Final-slides.pdf
18. https://docs.fcc.gov/public/attachments/DOC-368981A1.pdf
19. https://datatracker.ietf.org/doc/html/rfc8224
20. https://support.google.com/phoneapp/answer/12027891?hl=en
21. https://blog.hiya.com/how-to-check-phone-numbers-for-spam-labels

22. https://ustelecom.org/best-practices-redress-requests/
23. https://www.bandwidth.com/support/en/articles/12823060-how-do-i-use-the-call-logs-page
24. https://www.voicespamfeedback.com/
25. https://callreporting.t-mobile.com/
26. https://spamalerts.verizon.com/vsf/bestPractices
27. https://autoattendant.io/
28. https://www.hiya.com/products/connect/number-registration
29. https://www.reportarobocall.com/trf/
30. https://consumercomplaints.fcc.gov/hc/en-us/articles/115002234203-Unwanted-Calls-Texts-Phone
31. https://firstorion.com/case-studies/the-ultimate-how-to-guide-business-number-registration
32. https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-releases-annual-do-not-call-registry-data-book
33. https://docs.fcc.gov/public/attachments/DOC-405219A1.pdf
34. https://cdn.atis.org/sti-ga.atis.org/2026/02/20165621/2025-STIGA-Public-Report-Final.pdf
35. https://docs.fcc.gov/public/attachments/FCC-21-105A1.pdf
36. https://docs.fcc.gov/public/attachments/FCC-24-135A1_Rcd.pdf
37. https://docs.fcc.gov/public/attachments/DA-26-72A1.pdf
38. https://developer.hiya.com/docs/guides/voice-protection/number-reputation/create-a-business
39. https://crtc.gc.ca/eng/phone/telemarketing/identit.htm
40. https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/tackling-scam-calls-and-texts
41. https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-TRUST-2021-PDF-E.pdf
42. https://ustelecom.org/the-industry-traceback-group-itg/call-labeling-and-blocking-points-of-contact/
43. https://autoattendant.io/articles/how-to-get-a-business-phone-number

THE PUBLISHER

About Auto Attendant

Auto Attendant gives a small business one phone number and a recorded menu that sends each caller to the right person. The call rings the mobile that person already carries, using their normal dialler and their normal mobile plan. Pricing is a single flat monthly fee for the whole company rather than a charge for each user, and there is no app, desk phone or hardware to install.

One number, one menu, the phones you already own

A caller dials the business number, hears a short greeting and chooses an option. Each option can ring one mobile, ring several at once so whoever is free answers first, or try people one after another in a set order. There is no limit on how many people sit on the receiving end, because nobody is billed per seat. Setup is done by the owner in a few minutes: pick a number, write the greeting, and point each option at a mobile.

What it deliberately is not

An auto attendant routes a call; it does not answer one. Nobody at Auto Attendant speaks to callers, and no AI stands in for a receptionist. A business that wants its calls handled, messages taken and appointments booked wants an answering service, which is a different product at a different price. A business that needs call recording, queues, agent dashboards or CRM integration wants a contact centre platform. Auto Attendant is for the case where the call should simply reach the right pocket.

Keeping personal numbers off the internet

The business number is the only number a caller ever sees. Personal mobile numbers are never displayed and never given out, which is what lets an owner put a number on a website, an invoice, a van or a Google Business Profile without handing a personal line to everyone who finds it. An existing advertised number can be ported across and kept, and the old line keeps working while the port is in progress.

Work with Auto Attendant

Visit Auto Attendant to see how it works, how it compares to a personal mobile, Google Voice and a full phone platform, and the current pricing.

Telephone number portability, emergency calling and caller-ID rules differ by country and change over time. Articles published here describe general practice and cite primary regulator and carrier sources; they are not a guarantee of any timeline, and they are not legal or regulatory advice for a specific business.

Website: https://autoattendant.io