

ROBOCALL MITIGATION PROGRAM DESCRIPTION

SIPNATE LLC

Legal Entity	SIPNATE LLC
FCC Registration Number (FRN)	0038865218
Business Address	548 Dandelion Dr, Saint Johns, FL 32259, United States
Principal / Officer	Tanner Gregg - Sole Member and Chief Executive Officer
RMD Compliance Contact	Tanner Gregg, Chief Executive Officer
Email	tanner.gregg@gmail.com
Telephone	+1 561 566 2499

Version 1.0 | Effective upon adoption and filing in the FCC Robocall Mitigation Database

This program applies to voice traffic originated, carried, or processed by SIPNATE LLC to the extent applicable to the provider role selected in its Robocall Mitigation Database (RMD) certification. The program is designed to prevent the use of SIPNATE LLC's services for illegal robocalls, unlawful caller-ID spoofing, fraud, impersonation, or other unlawful calling activity and to support prompt traceback and remediation.

The formal STIR/SHAKEN implementation status selected in SIPNATE LLC's RMD filing controls for certification purposes. This document describes the company's mitigation practices and does not, by itself, make a separate representation regarding ownership of a particular STIR/SHAKEN certificate.

1. Governance and Compliance Responsibility

The Chief Executive Officer is responsible for oversight of the robocall mitigation program. Day-to-day compliance functions include customer due diligence, caller-ID authorization controls, traffic review, complaint and traceback handling, escalation, and suspension or termination decisions.

- SIPNATE LLC maintains a designated RMD contact who is expected to be reachable for FCC, law-enforcement, industry traceback, carrier, and downstream-provider inquiries.
- The company reviews this program when its services, network relationships, regulatory obligations, or risk profile materially change.
- Material changes to information reported in the RMD are reviewed for timely update in accordance with applicable FCC rules.

2. Know-Your-Customer (KYC) and Onboarding Controls

SIPNATE LLC takes affirmative measures to know new and renewing customers and to reduce the risk that its services are used to originate illegal traffic. The level of diligence is risk-based and may be enhanced for high-volume origination, unusual traffic profiles, newly formed entities, inconsistent ownership information, or other risk indicators.

- Collect and verify the customer's legal name, business address, contact information, service-use case, and responsible person.
- Obtain and review business formation records, tax/business identifiers, government-issued identification of an authorized principal when appropriate, and other records reasonably necessary to validate identity.
- Review the customer's expected call types, estimated volumes, calling geographies, target destinations, and the source and authorization status of telephone numbers used for caller ID.
- Require accurate information and prohibit anonymous, misleading, fictitious, or materially inconsistent onboarding data.
- Conduct enhanced review before enabling or materially increasing high-volume origination where risk factors warrant additional diligence.
- Re-screen or re-verify customers when ownership, contact information, traffic behavior, payment behavior, or complaint history creates a material risk signal.

3. Contractual and Acceptable-Use Requirements

Customers are required to use SIPNATE LLC services only for lawful purposes and to comply with applicable federal and state calling, caller-ID, consumer-protection, consent, and do-not-call requirements.

- Illegal robocalls, scams, fraud, impersonation, harassment, unlawful spoofing, and misrepresentation of calling identity are prohibited.
- Customers must use only calling numbers that they own, control, have been assigned, or are otherwise authorized to present.
- Customers must provide supporting documentation for number authorization when requested.
- SIPNATE LLC reserves the right to restrict traffic, reduce capacity, suspend service, or terminate service promptly when illegal or suspicious activity is identified or when a customer fails to cooperate with an investigation.

4. Caller-ID Authorization and STIR/SHAKEN Controls

SIPNATE LLC supports caller-ID authentication consistent with the STIR/SHAKEN framework where applicable. Traffic presented for A-level attestation is limited to circumstances in which there is a reasonable basis to know the customer and to verify that the customer is authorized to use the calling number.

- A-level attestation is not treated as a customer-selected label; it is conditioned on identity and calling-number authorization.
- SIPNATE LLC may require proof of number assignment, ownership, control, or a valid letter of authorization before a number is approved for caller-ID presentation.
- Caller-ID values that are invalid, malformed, clearly unauthorized, or inconsistent with the approved customer profile may be rejected, blocked, or investigated.
- Where the technical signing function is performed through an authorized service arrangement, SIPNATE LLC requires the signing process to be consistent with the provider's applicable STIR/SHAKEN obligations and the attestation basis supported by the underlying customer and number validation.
- SIPNATE LLC does not knowingly permit customers to use A-attestation to disguise the origin of unlawful traffic or to impersonate persons or businesses.

5. Traffic Monitoring and Analytics

SIPNATE LLC monitors traffic using internal operational data and signals received from interconnected providers. The company does not rely on a separately contracted third-party robocall analytics platform as the sole basis of its mitigation program; upstream or downstream providers may independently use their own analytics systems.

- Review of call detail records (CDRs), SIP signaling, caller-ID values, attestation information where available, call volumes, call-duration patterns, answer patterns, and destination patterns.
- Monitoring for sudden traffic spikes, high concentrations of short-duration calls, repeated use of unapproved calling numbers, sequential or high-velocity calling patterns, complaint spikes, and other behavior inconsistent with the approved use case.
- Review of carrier notices, downstream-provider feedback, blocking reports, traceback requests, consumer complaints, and law-enforcement or regulatory inquiries as risk signals.
- Risk-based escalation may include customer outreach, documentary re-verification, number re-verification, traffic sampling, rate limiting, route restriction, suspension, or termination.
- SIPNATE LLC will update this plan and the RMD filing as required if it later engages a third-party analytics vendor directly or materially changes its analytics practices.

6. Invalid, Unallocated, Unassigned, and Unauthorized Calling Numbers

SIPNATE LLC seeks to prevent the origination of traffic using caller-ID numbers that are invalid, unallocated, unassigned, or otherwise unauthorized for the originating customer.

- Calling-number authorization is associated with the customer's approved account or service profile.
- Use of emergency numbers, government numbers, financial-institution numbers, or other high-risk identities as caller ID without demonstrable authorization is prohibited.
- When credible evidence indicates that a calling number is being spoofed or misused, SIPNATE LLC may block or remove the number from the customer's authorized calling-number set pending review.

7. Know-Your-Upstream Provider and Interconnection Controls

SIPNATE LLC conducts reasonable due diligence on directly interconnected or upstream voice providers used to exchange covered traffic.

- Before establishing or renewing material voice relationships, SIPNATE LLC verifies provider identity, business contact information, and relevant regulatory information.
- Where required by FCC rules, SIPNATE LLC checks the Robocall Mitigation Database status of directly upstream domestic voice providers before accepting traffic from them.
- SIPNATE LLC expects interconnected providers to maintain appropriate robocall mitigation, traceback cooperation, and caller-ID authentication practices applicable to their role.

- Material compliance concerns, RMD removal, persistent traceback failures, or credible evidence of illegal traffic may result in route restrictions, suspension, or termination of the provider relationship.

8. Complaints, Tracebacks, and Investigations

SIPNATE LLC treats credible complaints, traceback requests, and regulatory or law-enforcement inquiries as priority compliance events.

- SIPNATE LLC commits to respond fully and within 24 hours to traceback requests from the FCC, law enforcement, and the registered industry traceback consortium, consistent with applicable FCC requirements.
- Traceback responses are coordinated through the designated RMD compliance contact and include available information sufficient to identify the relevant customer, upstream/downstream provider, route, and call record, subject to applicable law.
- SIPNATE LLC cooperates with the FCC, law enforcement, the industry traceback consortium, and interconnected providers in investigating and stopping illegal robocallers.
- A traceback or credible complaint may trigger immediate preservation of relevant records and a risk review of the customer or provider involved.
- Repeated complaints, non-cooperation, false information, or credible evidence of illegal calling may result in immediate suspension or termination.

9. Remediation, Suspension, and Termination

When SIPNATE LLC identifies potentially illegal or high-risk traffic, it uses a graduated or immediate-response process depending on severity.

- Investigate the traffic and compare it against the approved customer profile, caller-ID authorization, call records, and available carrier or traceback information.
- Request supporting documentation or an explanation from the customer when appropriate.
- Apply technical or commercial controls such as caller-ID restriction, rate limiting, destination restriction, traffic blocking, or temporary suspension.
- Terminate service without delay when SIPNATE LLC determines that the customer is knowingly engaged in illegal robocalling, fraudulent spoofing, or refuses to cooperate with a legitimate investigation.
- Where appropriate, notify affected upstream or downstream providers and preserve evidence relevant to traceback or enforcement.

10. Records and Documentation

SIPNATE LLC maintains records reasonably necessary to demonstrate and operate its mitigation program. Records may include onboarding and KYC materials, number-authorization evidence, customer compliance communications, call detail records, complaint records, traceback responses, escalation notes, and suspension or termination actions.

- Records are retained for a period reasonably sufficient to support traceback, regulatory compliance, contractual obligations, and investigations, and for longer periods when required by applicable law or a preservation request.
- Access to sensitive customer and compliance records is limited to personnel or service providers with a legitimate business or legal need.

11. Training and Internal Accountability

- Personnel or contractors involved in customer onboarding, voice operations, or compliance are instructed to escalate suspicious traffic and not to override mitigation controls for commercial reasons.
- The compliance contact may require additional verification, suspend onboarding, reduce traffic privileges, or direct an immediate service suspension when risk warrants.
- Material failures or recurring control gaps are reviewed and corrective measures are documented.

12. Continuous Review and RMD Maintenance

SIPNATE LLC reviews the effectiveness of this program on an ongoing basis and adjusts controls in response to changes in traffic, complaints, traceback experience, carrier feedback, regulatory requirements, and emerging fraud techniques.

- RMD information is reviewed for accuracy when material company, contact, ownership, provider-role, STIR/SHAKEN, analytics, or mitigation information changes.
- SIPNATE LLC will update its RMD filing within the applicable FCC deadline when required information changes and will complete required annual recertification.
- The company will not knowingly allow the continued use of its services by a customer or provider whose conduct is inconsistent with this program.

13. Program Certification and Adoption

SIPNATE LLC adopts the practices described in this Robocall Mitigation Program Description as its operational framework for preventing and addressing illegal robocalls and unlawful caller-ID spoofing. The company intends this program to be read together with the certifications and provider-role selections made in its FCC Robocall Mitigation Database filing.

SIPNATE LLC will take reasonable steps to avoid originating or facilitating illegal robocall traffic, will maintain know-your-customer and applicable upstream-provider diligence, will use traffic monitoring and escalation controls, and will cooperate promptly with traceback and enforcement efforts.

Approved for SIPNATE LLC by	Tanner Gregg
Title	Sole Member and Chief Executive Officer
RMD Compliance Email	tanner.gregg@gmail.com
RMD Compliance Telephone	+1 561 566 2499
Effective Date	Effective upon adoption and filing

Regulatory framework

This program is structured to address the mitigation-plan and traceback obligations applicable to RMD filers, including 47 C.F.R. §§ 64.1200(n) and 64.6305, as applicable to SIPNATE LLC's selected provider role.

Analytics Vendor Disclosure

At the time of filing, SIPNATE LLC does not directly contract with a separate third-party robocall analytics vendor. SIPNATE LLC relies on internal operational review and signals received from interconnected providers. If this changes, SIPNATE LLC will update its mitigation program and RMD filing as required.