

GATED NETWORKS, INC.

Robocall Mitigation Plan

Navigate™ | Universal Branding Gateway Service

Status: Version 1.1 Filing Version

Filing date: September 10, 2026

1. Filing entity

Legal name: Gated Networks, Inc.

Jurisdiction and form: Delaware corporation

Formation date: July 8, 2022

Principal business address: 2686 Firebush Lane, Naples, Florida 34105

FCC Registration Number: 0038664199

OCN: 266H

Website: <https://gatednetworks.com>

RMD provider category: Non-gateway intermediate provider — adopted as Gated's reasonable, good-faith working classification for the Navigate™ call-branding gateway service; no definitive FCC classification ruling has been issued for Gated's Navigate signaling-only architecture.

Gated Networks, Inc. ("Gated") has no registered DBA. This filing concerns Gated's new Navigate service offering. **Navigate™** is a pending trademark of Gated Networks. In addition to the Navigate service, Gated also operates the BCID Platform under contract with the CTIA "The Wireless Association" within the CTIA's Branded Calling ID ("BCID") ecosystem. BCID™ is a trademark of CTIA and its wholly owned subsidiary BCID LLC.

2. Status and scope of this plan

Navigate is a cloud-hosted **call branding gateway service** offered by Gated Networks, Inc. It enables enterprise customers operating outside the United States, through participating originating service providers (OSPs), to obtain access to the benefits of verified call branding made available by U.S. carriers participating in CTIA's Branded Calling ID (BCID) ecosystem. Navigate combines independent enterprise vetting, deterministic call-authentication eligibility controls, SHAKEN signing, and conveyance of vetted branding information for eligible calls intended for recipients served by participating U.S. providers.

As of the filing of this amended plan, Gated has completed implementation of the STIR/SHAKEN authentication framework for the Navigate service. Gated has:

- completed the FCC and industry registrations required for its service;

- obtained its own Service Provider Code token from the STIR/SHAKEN Policy Administrator on August 31, 2026;
- used its SPC token to obtain its own production STI certificate from the CTIA STI-CA operated by SecureG;
- completed the STI-PA and production-readiness testing required for its implementation;
- configured and tested its authentication, attestation, certificate-security, logging, and access-control functions;
- verified that the independent Vetting Agents on which Navigate will rely have current authorization and contractual standing under both the CTIA BCID and GSMA OVC Vetting-Agent frameworks; and
- activated the operational monitoring, incident-response, traceback, suspension, and record-retention procedures required for production service.

Gated has not yet launched the planned Navigate trial and is not presently processing production Navigate calls. This planned pre-launch period does not reflect an incomplete STIR/SHAKEN implementation: Gated holds the credentials and operates the technical and procedural controls needed to authenticate every call covered by its current implementation obligation when the trial begins. The implemented service subjects every call-signaling transaction it processes to this mitigation program, including requests that do not result in a signed Identity value. If a required verification fails, Gated does not create or return a signed Identity value. Gated's refusal to authenticate does not block the underlying call; the originating service provider retains responsibility for routing, media, and call completion.

3. Service and network architecture

3.1 Gated's function

The term **call branding gateway** describes Navigate's commercial and functional role as an access point between international enterprises and the BCID verified-branding ecosystem. It is not intended to assert that Gated is a “gateway provider” as that term is defined by the FCC. Under the current architecture, Gated returns authenticated signaling to the same OSP and does not transmit the call downstream to another U.S. provider. For RMD purposes, Gated is proceeding under the separately stated good-faith working assumption that **Navigate is a non-gateway intermediate-provider service**.

No enterprise is eligible to participate or have its calls authenticated until its identity, telephone-number associations, and applicable display-identity claims have been vetted by an independent Vetting Agent that is contractually authorized and obligated under both the CTIA BCID and GSMA OVC Vetting-Agent frameworks.

For each requested authentication transaction:

- An independent, duly authorized Vetting Agent verifies the enterprise and approves the applicable identity and telephone-number claims under the CTIA BCID and GSMA OVC Vetting-Agent contractual requirements.

- The independently vetted enterprise originates a call through its OSP (registered and pre-approved by Navigate) using a secure connection controlled by the OSP.
- The OSP submits a Branding Request by sending Navigate a SIP INVITE that identifies the originating enterprise through its Enterprise ID (EID).
- Navigate receives the SIP INVITE over a mutual TLS connection at its AWS-hosted service and verifies the submitting OSP by matching the request's source IP address against the source IP address pre-authorized for that OSP.
- Navigate verifies that the enterprise's independent vetting remains active and evaluates the OSP, EID, originating telephone number, Vetting Agent authorization, and applicable vetted identity claims.
- If every applicable control succeeds and the call is eligible for authentication, Navigate creates a SHAKEN PASSporT including vetted enterprise RCD claims using Gated's attestation decision, SPC, private signing key, and STI certificate.
- Navigate returns a SIP 302 response to the same OSP. The private Gated-OSP interface conveys the SIP Identity header containing a signed SHAKEN PASSporT with vetted enterprise RCD claims in that response.
- The OSP copies the returned SHAKEN PASSporT, without modification, into the outbound SIP INVITE and transmits the call toward its selected downstream provider.

In this plan, the terms "gateway" and "branding gateway" are used only in the ordinary commercial sense and do not describe FCC-defined gateway-provider status.

3.2 Functions Gated does not perform

Gated does not:

- contract with end users to furnish voice communications;
- assign, lease, or resell telephone numbers;
- carry or process call audio or other media;
- select the downstream U.S. provider;
- transmit the call to a downstream provider;
- provide PSTN routing or call completion;
- invoice an end user for voice calling; or
- control whether the OSP completes an unauthenticated call.

Audio passes directly between the OSP and the providers in the downstream call path. Gated's involvement is limited to the authentication transaction and related identity, security, audit, and compliance functions.

3.3 Infrastructure and third parties

Gated operates and controls its service in Amazon Web Services. AWS supplies cloud infrastructure, but Gated controls authentication policy, eligibility decisions, signing logic, access controls, and operational decisions.

The service also depends on:

- CTIA, which administers the BCID ecosystem and trust model through a wholly owned subsidiary BCID, LLC.
- the CTIA STI-CA operated by SecureG, which has issued Gated's production STI certificate;
- independent Vetting Agents that are contractually authorized and obligated under both the CTIA BCID Vetting-Agent framework and the GSMA Open Verifiable Calling (OVC) Vetting-Agent framework; and
- participating OSPs, which identify the enterprise source of each call and provide the EID in the SIP INVITE.

4. Authentication Role

Navigate is IP-based. Under its stated working assumption, Gated acts as the authenticating provider for calls it signs and performs the authentication functions described in this plan. Gated adopts this position because Gated independently applies the EID/TN/OSP authorization controls, determines whether authentication is permitted, assigns A-level attestation to eligible calls displaying NANP originating telephone numbers, and uses its own SPC token, private key, and STI certificate. The OSP supplies source facts and remains responsible for securely knowing the call's origin, but it does not make Gated's authentication or attestation decision.

Authentication-role status: As of the filing of this amended plan, Gated has fully implemented the STIR/SHAKEN authentication framework for the Navigate service. Gated obtained its own SPC token from the STIR/SHAKEN Policy Administrator on August 31, 2026, used that token to obtain its own production STI certificate from the CTIA STI-CA operated by SecureG, and completed the testing and production-readiness work required for its implementation. Gated no longer relies on the implementation extension in 47 CFR § 64.6304(b). Gated has not yet launched the planned Navigate trial and is not presently processing production Navigate calls.

Gated will use its own SPC token, private signing key, and STI certificate to authenticate each qualifying Navigate call for which it assumes the non-gateway intermediate-provider authentication obligation. Gated makes the authentication and attestation decision and preserves authenticated caller-identification information without alteration except where removal is permitted by the FCC's rules. When the planned trial begins, all calls covered by Gated's current implementation obligation will be processed in accordance with 47 CFR § 64.6302.

5. OSP approval, authentication-security, and abuse-prevention

Gated provides Navigate branding gateway services only to approved OSPs operating under the Navigate Platform Participation Agreement. The Participation Agreement establishes the OSP's contractual obligations within the solution. At a minimum, the agreement requires the OSP to:

- execute a role-specific Participation Order and be approved by Gated for the OSP role;
- know the identity of the Enterprise originating each Branding Request;
- submit each Branding Request only on behalf of the applicable Enterprise associated with the referenced EID;
- ensure that information it submits through the platform APIs is accurate, complete, and timely;
- perform its approved role in accordance with the Agreement, and applicable Navigate platform procedures;
- maintain the licenses, authorizations, approvals, registrations, certifications, and other qualifications required for its role; and
- accept Gated's right to reject invalid or improperly formatted transactions and to suspend access when reasonably necessary to respond to fraud, abuse, unauthorized use, or a material risk to the Platform or other Participants.

The Agreement also provides indemnification protection for inaccurate, incomplete, unauthorized, or unlawful information submitted by or on behalf of a Participant and permits termination for an uncured material breach.

As a condition of production activation, Gated requires each OSP to maintain a secure connection to each participating enterprise and to the Navigate platform; accurately pass the identity of the calling enterprise to the Navigate Platform; preserve the returned Identity header value without modification; and maintain consistency between the PASSporT and outbound INVITE. Gated will not activate an OSP for Navigate production service until the OSP has accepted these obligations in the controlling contractual documents.

The Navigate contractual documents distinguish independent enterprise vetting from Gated's per-request authentication controls. The OSP submits each Branding Request as a SIP INVITE over mutual TLS from a pre-approved source IP address. Navigate authenticates the connection and OSP, verifies the applicable independently vetted claims, and applies the deterministic EID/TN/OSP eligibility controls before Gated makes the authentication and attestation decision.

Before activation, Gated requires every prospective OSP to be vetted by a CTIA-approved Vetting Agent. The Vetting Agent verifies and documents the OSP's legal identity, jurisdiction, business address, authorized representative, and technical contacts. Each OSP undergoes full reverification by a CTIA-approved Vetting Agent at least annually and upon a material ownership, regulatory, security, contact, service, or traffic change.

After identity vetting, Gated personnel perform the technical onboarding review. Gated validates and records the OSP's approved source IP address and establishes the mutual-TLS credentials required to

submit SIP INVITEs to Navigate. Gated activates the OSP only after both the Vetting Agent review and Gated's technical review have been completed successfully.

Gated monitors each approved OSP after activation. Gated immediately suspends or restricts signing access when an OSP submits requests from an unauthorized endpoint; refuses traceback or regulatory cooperation; or otherwise creates an unacceptable authentication or public-safety risk. David Peek, Chief Technology Officer, has emergency-suspension authority. When immediate suspension is not required, Gated may provide notice and a reasonable cure period consistent with the Participation Agreement. Reinstatement requires documented remediation, successful retesting, and written approval from Douglas Ranalli, Chief Executive Officer.

Gated will update its filing and compliance program if controlling FCC guidance requires different treatment of Navigate.

6. Enterprise identity and telephone-number vetting

Independent enterprise vetting is a mandatory, threshold control for Navigate. Every participating enterprise must complete vetting through an independent Vetting Agent before Gated will activate the enterprise, accept its EID as eligible for authentication, or sign a call on its behalf. The Vetting Agent must be contractually authorized and obligated under both the CTIA BCID Vetting-Agent framework and the GSMA OVC Vetting-Agent framework. Neither an OSP's assertion that it knows the enterprise nor Gated's technical onboarding review substitutes for this independent vetting.

The independent Vetting Agent establishes the enterprise's identity and entitlement claims. Gated separately determines, at the time of each signing request, whether the vetted claims remain active and whether the OSP, EID, originating TN, and requested identity attributes satisfy Navigate's deterministic authorization controls. This separation provides independent identity proofing followed by Gated-controlled, transaction-specific enforcement.

The applicable vetting process establishes and maintains evidence concerning:

- the enterprise's legal identity;
- the authority of the enterprise representative;
- the enterprise's right to use its registered Caller Display Name and Call Logo;
- the enterprise's association with each originating telephone number;
- the accuracy and appropriateness of the Caller Display Name, Call Logo, and Call Reason;
- material fraud, impersonation, sanctions, government-control-list, and adverse-risk indicators; and
- current approval, suspension, expiration, or revocation status.

Gated will accept a vetting result only from an independent Vetting Agent on Gated's approved-issuer list whose required CTIA BCID and GSMA OVC authorizations and contractual status are current.

7. Per-call authentication controls

Gated uses a fail-closed policy for authentication. For calls displaying NANP originating telephone numbers that are eligible under the U.S. STIR/SHAKEN framework, Gated creates and returns an A-attested SHAKEN PASSporT with calling-party RCD identity claims (e.g., name, logo, and call reason) only when all required checks succeed.

For every signing request, Gated verifies that:

- the SIP INVITE arrived over a successful mutual TLS connection from the source IP address pre-authorized for the submitting OSP;
- the OSP supplied an EID;
- the enterprise completed the required independent vetting through a Vetting Agent contractually authorized and obligated under both the CTIA BCID and GSMA OVC Vetting-Agent frameworks;
- the Vetting Agent remains authorized and the applicable vetting result has not expired, been suspended, or been revoked;
- the EID is active, verified, and not suspended or revoked;
- the originating TN in the INVITE is on the active, independently validated TN list for that EID;
- the submitting OSP is authorized for that specific EID/TN combination;
- the requested Caller Display Name, Call Logo, and Call Reason are active independently vetted claims for the EID;

If any required check fails, Gated does not create or return a signed Identity value. The particular SIP response or error treatment may vary by failure class under Gated's controlled interface specification, but no failure response shall contain a Gated-signed SHAKEN PASSporT.

Gated's PASSporT uses `ppt=shaken` and, for eligible BCID calls, contains only vetted RCD. Gated will include an `rcdi` integrity value whenever external logo content is referenced. Gated will enforce current ecosystem content and size restrictions.

8. Authentication of Calls Displaying both NANP and Non-NANP Originating Telephone Numbers

A principal purpose of Navigate is to extend verified enterprise identity and branded-calling protections to lawful international calls delivered to recipients in the United States. Navigate is designed to support eligible calls displaying valid and properly authorized U.S. NANP and non-NANP E.164 originating telephone numbers.

Gated plans to begin trial service in September 2026 with calls displaying properly assigned U.S. NANP originating telephone numbers. Gated will provide results from this phase to participating terminating service providers and the STI-GA and will use their feedback to evaluate the trial's authentication, verification, branded-calling, interoperability, and consumer-protection results.

Subject to the results of the initial phase, Gated intends to evaluate a subsequent trial phase involving calls displaying properly authorized non-NANP E.164 originating telephone numbers. Any such trial will be limited to calls terminating with U.S. service providers that have affirmatively requested in writing that Gated commence testing calls displaying non-NANP originating telephone numbers. The trial will be conducted on a controlled basis using independently verified TN right-to-use information and call-level records sufficient to support traceback, audit, and evaluation.

For both U.S. NANP and non-NANP E.164 originating telephone numbers, an independent vetting agent will verify the calling enterprise's identity and right to use each originating telephone number. The vetting procedures will be aligned with applicable GSMA OVC and CTIA BCID vetting policies and contractual requirements.

Gated has presented the Navigate service and its proposed implementation to the STI-GA Board of Directors and Board leadership. Gated has also briefed the STI-GA Technical Committee. Discussions with the STI-GA are ongoing. Gated will monitor changes to applicable FCC rules, STI governance requirements, and participating service-provider requirements. If a controlling requirement changes, Gated will conform its implementation and update its Robocall Mitigation Database filing as required.

9. Signaling security and certificate controls

Gated has implemented controls appropriate to the sensitivity of its signing function, including:

- authenticated and encrypted OSP connections;
- mutual TLS authentication combined with OSP-specific source-IP authorization;
- least-privilege access to signing and administrative functions;
- separation of production, test, and development environments;
- protected key generation, storage, use, rotation, backup, and destruction;
- prohibition on exporting or sharing private signing keys with unauthorized parties;
- certificate status and revocation monitoring;
- immediate suspension of signing following suspected key compromise;
- logging and alerting for unauthorized access, repeated denials, and policy overrides;
- change control for signing logic and attestation policy;

David Peek, Chief Technology Officer, has documented and approved the implemented key-management architecture, access-control system, logging and security-monitoring configuration, vulnerability-management process, incident-response process, backup controls, and responsible operational roles. Launch-readiness testing has verified these controls, and Gated retains the approval and test evidence for seven years. Gated does not represent a security control as operational until it has been implemented and tested.

10. Authentication-service monitoring and response

Because Gated does not carry media or route the outbound call, its monitoring focuses on signaling and use of its authentication service.

In addition to applying its deterministic eligibility controls to each request, Gated reviews denied requests, invalid or revoked credentials, unauthorized submitting endpoints, traceback requests, complaints, and other credible evidence of misuse. Gated does not use call analytics or a third-party analytics vendor to identify or block illegal calls.

Gated's available remedies include refusing an individual signing request; increasing review; restricting an OSP, EID, TN, credential, or endpoint; suspending signing access; revoking platform credentials; preserving evidence; notifying appropriate ecosystem participants; and terminating the OSP's access.

Gated does not block the underlying call. When Gated refuses authentication, the OSP remains responsible for deciding whether and how the call proceeds.

Call-analytics and volume-baseline disclosure: Gated does not use call analytics or a third-party analytics vendor to identify or block illegal calls. Because Navigate is a new service and anticipated traffic can change rapidly, Gated does not establish fixed expected-volume baselines for each OSP. Gated instead applies deterministic authentication-eligibility controls to every call-signaling transaction.

11. Traceback and cooperation

Under its good-faith non-gateway intermediate-provider classification assumption, Gated cooperatively participates with the Industry Traceback Group, responds fully and within 24 hours to traceback requests from the FCC, law enforcement, and the Industry Traceback Group, and cooperates in investigating and stopping illegal calls that use or attempt to use Gated's service.

Gated has not previously received a traceback request through the Industry Traceback Group's Secure Traceback Portal. Gated's RMD filing is public, and Gated maintains current traceback contact information and operational readiness to receive, investigate, and answer requests. Gated will complete any portal enrollment or recipient registration made available by the Industry Traceback Group.

11.1 Confirmation Detail Record

The Navigate platform generates and retains a Confirmation Detail Record for every successfully confirmed call. This record is distinct from a conventional carrier call detail record and is referred to in this plan as a "Confirmation Detail Record."

For an authenticated transaction, Navigate generates a unique cryptographic signature "SIG" associated with the signed PASSporT. The terminating service provider (TSP) returns that SIG to the Navigate platform through its `confirm passing` API call. When the returned SIG matches the unique SIG associated with the signed PASSporT, the platform generates the Confirmation Detail Record. The record therefore documents the association between the Navigate authentication transaction and the TSP's confirmation that the call passed through the participating call path.

Each Confirmation Detail Record contains:

- Enterprise ID (EID);
- Display Identity Record ID (DIRID);
- Originating Service Provider ID (OSP-ID);
- Onboarding Agent ID (OA-ID);
- Vetting Agent ID (VA-ID);
- Terminating Service Provider ID (TSP-ID);
- PASSporT issuance time (*iat*); and
- originating telephone number (*orig-TN*).

Together, these data identify every Navigate participant associated with the confirmed call and point to the specific vetted Display Identity Record used when Gated generated the SHAKEN PASSporT. This permits a traceback responder to identify the originating provider and enterprise, the onboarding and vetting participants, the terminating provider that confirmed passage, and the vetted identity claims associated with the call.

The Participation Agreement calls a successfully matched TSP Confirmation a "Matched Confirmation" and makes Matched Confirmations the authoritative transaction records for reporting and settlement. It authorizes Gated to maintain Branding Requests, Confirmations, settlement records, audit records, and other operational information for operational, regulatory, security, audit, and related purposes. Gated's controlled technical specifications define the Confirmation Detail Record, SIG-matching process, and record fields, and Gated's retention policy establishes the seven-year retention period.

The records are stored in Amazon Web Services and are encrypted both in transit and at rest. Data stored in Amazon S3 is protected using Amazon S3 server-side encryption with Amazon S3-managed keys (SSE-S3) using AES-256-GCM. Encryption at rest is applied to the AWS storage containing the records; each individual record is not separately encrypted. The encryption keys used for data protection are separate from and unrelated to Gated's SHAKEN private key used for call authentication. Access to AWS cloud services is restricted through company-defined roles to authorized Gated personnel with applicable job responsibilities. Gated applies multi-factor authentication and regular password-management and update requirements to cloud access. All fields contained in Confirmation Detail Records are searchable, allowing authorized personnel to locate records using any recorded participant identifier, identity-record identifier, originating telephone number, or issuance time.

11.2 Signing Confirmation Record

When Navigate does not receive a matching TSP Confirmation, it generates and retains a Signing Confirmation Record containing the information known when the call was signed: EID, DIRID, OSP-ID, OA-ID, VA-ID, PASSporT issuance time (*iat*), and originating telephone number (*orig-TN*).

The Signing Confirmation Record identifies the enterprise, vetted identity, originating number, and originating, onboarding, and vetting participants. It does not contain a TSP-ID because Navigate did not receive a matching confirmation identifying a participating terminating provider.

A mismatched SIG, timeout, or other failure to receive a valid matching TSP Confirmation does not produce a Confirmation Detail Record. The Signing Confirmation Record remains Gated's record of the signing event.

11.3 Denied requests

Navigate generates log entries for requests that fail an authentication-eligibility control and are denied before a PASSporT is signed. These logs provide evidence that the platform applied its fail-closed policy.

Access to these records is limited to the Chief Technology Officer and designated Gated operational, security, compliance, and traceback-support personnel whose assigned duties require access. Changes to historical records are captured in access-controlled audit logs.

12. Complaints, investigations, and remediation

Gated will promptly investigate credible evidence that its service has authenticated or may authenticate illegal, spoofed, fraudulent, or unauthorized calls.

Depending on severity, David Peek, Chief Technology Officer, may immediately suspend an OSP, EID, TN, credential, or endpoint before completion of an investigation when reasonably necessary to protect the integrity of Gated's authentication service, participants, or the public. Gated documents the allegation or triggering event, evidence reviewed, scope and time of suspension, interim controls, notifications, investigation findings, remediation, testing, reinstatement decision, and final disposition.

Suspended access may be reinstated only with the documented approval of Douglas Ranalli, Chief Executive Officer, after the underlying issue has been remediated, relevant controls have been successfully retested, and the evidence supports a determination that reinstatement does not create an unacceptable robocall, authentication, security, or compliance risk. Reinstatement documentation identifies the corrective measures, test results, any conditions or enhanced monitoring, approving officer, and effective date.

13. Governance, oversight, and updates

Gated's Chief Executive Officer is accountable for the robocall-mitigation program. The Chief Technology Officer is responsible for implementation, incident review, vendor oversight, policy updates, and the accuracy of the company's RMD filing.

13.1 Quarterly governance review

Gated has established a Robocall Mitigation Governance Committee consisting of the Chief Executive Officer, Chief Technology Officer, and President. The Committee meets quarterly and before any material RMD certification when appropriate. It reviews a documented dashboard addressing:

- Confirmation Detail Records, Signing Confirmation Records, unmatched Confirmations, and material failure reasons;
- traceback requests and response times;

- complaints, suspected abuse, investigations, and remediation;
- restrictions or suspensions involving an OSP, EID, TN, credential, endpoint, or participant;
- security incidents, access-control changes, and certificate events;
- material platform, contract, policy, vendor, or regulatory changes;
- events that may require an RMD update; and
- open corrective actions, owners, and due dates.

The Committee maintains minutes recording the information reviewed, decisions reached, approvals given, and corrective actions assigned. A quarter with no exceptions is documented as such.

13.2 Monthly operational oversight

The Chief Technology Officer produces or reviews a monthly operational report covering the foregoing service, control, security, incident, and response metrics. Material exceptions are escalated promptly to the Chief Executive Officer rather than held for the next quarterly meeting.

13.3 Traceback exercises

Gated conducts a traceback and record-retrieval exercise annually. The exercise tests dedicated-email intake, Zendesk ticket creation, assignment, escalation, record retrieval, participant identification, evidence preservation, and preparation of a complete response within 24 hours.

13.4 OSP and Vetting Agent oversight

Gated reviews participating OSPs and independent Vetting Agents annually, and upon a material risk event. Vetting Agent oversight includes confirming continued authorization and contractual standing under both the CTIA BCID and GSMA OVC Vetting-Agent frameworks. Findings and any restrictions, remediation, suspensions, or terminations are documented. If a Vetting Agent loses a required authorization or contractual standing, Gated suspends reliance on that Vetting Agent's results pending documented review and resolution.

13.5 Independent assurance and annual assessment

Gated obtains the annual independent SOC 1 Type II and SOC 2 Type II assurance described in the Navigate Platform Participation Agreement. Management reviews relevant findings, determines their effect on the robocall-mitigation program, assigns remediation, and tracks remediation to closure. Gated also performs an annual management assessment of the controls and supporting records described in this plan.

13.6 RMD change management and annual recertification

Gated will update its RMD filing within ten business days of a reportable change and will recertify annually on or before March 1. The annual review will reconfirm the company's ownership, contact information, authentication status, mitigation controls, traceback procedures, and the accuracy of this plan.

14. Enforcement and investigation history

Based on an inquiry confirmed by Douglas Ranalli, Chief Executive Officer, on July 16, 2026, neither Gated nor any entity sharing Gated's ownership, management, directors, or control has, during the preceding two years, been the subject of a formal FCC, law-enforcement, or regulatory action or investigation involving illegal robocalls, spoofing, facilitation of illegal calls, or a deficient RMD filing or mitigation program.

15. Responsible contact

Robocall-mitigation contact: David Peek

Title and department: Chief Technology Officer

Business address: 2686 Firebush Lane, Naples, Florida 34105

Telephone: 603-289-9096

Email: support@gatednetworks.com

Support routing: The dedicated email address automatically routes messages to Gated support personnel.

16. Officer review and certification support

Douglas Ranalli, Chief Executive Officer, is Gated's certifying officer.

Gated's disclosed principals are Douglas J. Ranalli, Chief Executive Officer (60%); David Peek, Chief Technology Officer (20%); and Shae Ranalli, President (10%). Douglas Ranalli and Shae Ranalli are Gated's corporate directors. The remaining 10% is held collectively by passive outside investors. No outside investor exercises management or supervisory responsibility or control over Gated, and the outside investors are not treated as additional RMD principals. Current FCC guidance does not require identification of every passive shareholder solely by reason of share ownership. Gated has no parent, subsidiary, affiliate, commonly controlled entity, or other related entity.

Gated intends to submit this plan publicly without requesting confidential treatment. The public plan describes controls at a level sufficient to explain the mitigation program while omitting private keys, credentials, source IP addresses, detailed security configurations, and other information that could create security risk.