

DIAGNOTES ROBOCALL MITIGATION PLAN

Business Information

Diagnotes, Inc., a subsidiary of
DrFirst.com, Inc.

Contact Information

David Brown
Associate General Counsel
Phone: 301.231.9510 3222
Email: dbrown@drfirst.com

1. COMPANY OVERVIEW

DrFirst.com, Inc. (“DrFirst”), which does business through its subsidiary “Diagnotes” is a healthcare technology company providing communication, telehealth, and secure messaging solutions to healthcare organizations. Diagnotes’ voice services enable licensed healthcare providers to contact patients while protecting provider privacy by displaying the healthcare organization’s main telephone number as the caller ID.

Role in Call Chain: Voice Service Provider (Originating)

Diagnotes, does not operate telecommunications network facilities. All voice traffic is resold from Bandwidth, Inc., a contracted voice API provider, which provides call origination, routing, and STIR/SHAKEN authentication. As a reseller or value-added service provider (“VASP”), Diagnotes does not have control over the network infrastructure facilities necessary to implement STIR/SHAKEN.

2. STIR/SHAKEN IMPLEMENTATION

Diagnotes does not operate telecommunications network facilities or originate calls directly to the PSTN. All calls are originated through Bandwidth’s Voice API. Bandwidth, as the originating carrier, applies STIR/SHAKEN authentication and signs calls in accordance with FCC requirements.

This arrangement ensures that all calls originated through Diagnotes’ platform receive STIR/SHAKEN authentication at the network level without requiring Diagnotes to operate its own telecommunications infrastructure.

3. KNOW YOUR CUSTOMER (KYC) PROCEDURES

3.1 Customer Onboarding (Healthcare Organizations)

Diagnotes' voice services are available exclusively to verified healthcare organizations. Before a customer can access voice functionality, Diagnotes performs the following verification steps:

- a) Contract Execution:** All customers must execute a written service agreement that includes terms governing acceptable use of voice services and compliance with applicable laws.
- b) Business Verification:** Diagnotes verifies that the customer is a legitimate healthcare organization (hospital, medical practice, hospice, etc.).
- c) Manual Enablement:** Diagnotes administrators must manually enable voice functionality for each customer account. Voice services are not automatically available and require explicit activation by Diagnotes staff.

3.2 End User (Healthcare Provider) Verification

Individual users who can initiate calls through Diagnotes' platform must meet all of the following requirements:

- a) Provisioning:** Users must be provisioned by the customer organization's account administrator through one of two methods: - Manual creation in the Diagnotes system by an authorized administrator, or - Automated provisioning via SAML integration with the customer's Identity Provider (Active Directory)
- b) Authentication:** Users must be signed in and authenticated before accessing calling features. Authentication is performed either through Diagnotes credentials or via the customer's enterprise Identity Provider.
- c) Permission:** Users must be explicitly granted calling permission by their organization's account administrator. This permission can be revoked at any time by the administrator.
- d) Staff Verification:** Customer healthcare organizations are contractually responsible for ensuring that only authorized, licensed personnel are provisioned with calling capabilities. Diagnotes relies on healthcare organizations to verify their own staff credentials, consistent with healthcare industry standards for provider credentialing.

3.3 Existing Customer Procedures

Diagnotes' KYC procedures have been in place and consistently applied since the launch of voice services approximately six years ago. All customers, regardless of onboarding date, are subject to the same verification requirements. No grandfathering or reduced verification applies to existing customers.

4. CALL MONITORING AND ANALYTICS

4.1 Third-Party Analytics Vendors

Diagnotes uses the following third-party vendors for call analytics and monitoring:

- a) Bandwidth, Inc.** - Role: Voice API provider and originating carrier - Services: Carrier-level analytics, call detail records, fraud detection capabilities, STIR/SHAKEN authentication
- b) Amazon Web Services (AWS) CloudWatch** - Role: Cloud monitoring and logging platform - Services: Anomaly detection, real-time alerting, API request logging, log analysis

4.2 Internal Monitoring Systems

In addition to third-party services, Diagnotes maintains internal monitoring capabilities:

- a) API Request Logging:** All API requests to initiate calls are logged via AWS CloudWatch, capturing request metadata, timestamps, and outcomes.
- b) Database Logging:** All call requests and callbacks are logged in Diagnotes' internal database, including: - Initiating user identity - Provider phone number - Patient phone number - Caller ID number displayed - Timestamp - Call outcome/status
- c) Anomaly Detection:** AWS CloudWatch alarms are configured to detect anomalous call volume patterns and alert operations staff when thresholds are exceeded.

4.3 Rate Limiting

Diagnotes enforces rate limiting on all call requests to prevent volume abuse and detect unusual activity patterns. Rate limits are applied at the API level to ensure no single user or customer can generate excessive call volume.

4.4 Only accepting Traffic from Providers that Have Files in the RMD

In accordance with FCC rules, because Diagnotes is a reseller of VoIP services and lacks the control over the network infrastructure necessary to implement STIR/SHAKEN, Diagnotes relies on Bandwidth, which is currently listed in the RMD, to only accept traffic from providers that at a minimum satisfy the requirements under 47 C.F.R. §§ 64.6305(g)(1)-(4).

5. REASONABLE STEPS TO MITIGATE ILLEGAL ROBOCALL TRAFFIC

Diagnotes has implemented the following affirmative measures to prevent customers from originating illegal robocall traffic:

5.1 Access Restrictions

- Voice services are restricted exclusively to verified healthcare organizations under contract with Diagnotes or its parent.

- Individual users must be authenticated and explicitly permissioned by their organization's administrator
- No API-based or automated mass calling capabilities are available to end users
- All calls must be initiated through Diagnotes-controlled application interface by an authenticated user
- No bulk dialing, auto-dialer, or predictive dialing functionality is provided

5.2 Volume Controls

- Rate limiting prevents high-volume calling from any single user or customer
- Anomaly detection via CloudWatch alerts identifies unusual call patterns
- Call volume is monitored at both the individual user and customer organization levels

5.3 Immediate Suspension Capability

Diagnotes can immediately suspend calling capabilities at multiple levels:

a) User Level: Individual user permissions can be revoked instantly by either Diagnotes' administrators or customer account administrators. Upon revocation: - Further call attempts receive HTTP 403 Forbidden response from the API - Calling interface is immediately removed from the user's application view - Suspension is logged for audit purposes

b) Customer Level: Voice functionality can be disabled for an entire customer organization at any time by Diagnotes administrators, immediately preventing all users under that account from initiating calls.

5.4 Comprehensive Logging

All call activity is logged with full metadata, enabling: - Complete audit trails for all calls placed through the platform - Rapid investigation of any reported abuse or suspicious activity - Timely and accurate response to traceback requests - Historical analysis of calling patterns

6. TRACEBACK RESPONSE PROCEDURES

Diagnotes commits to responding to all traceback requests within 24 hours of receipt.

Traceback Response Process:

1. **Receipt and Acknowledgment:** Upon receiving a traceback request from an authorized source (Industry Traceback Group, FCC, law enforcement, or other voice service provider), Diagnotes will acknowledge receipt and begin investigation.
2. **Investigation:** Diagnotes will query internal call logs to identify:
 - The originating user
 - The customer organization
 - Complete call metadata (numbers involved, timestamp, caller ID used)
 - User authentication and permission status at time of call

3. **Response:** Diagnotes will provide the requesting party with relevant call information within 24 hours.
 4. **Enforcement Action:** If a traceback identifies illegal or unwanted robocalling activity originating through Diagnotes' platform:
 - The user's calling permissions will be immediately suspended
 - The customer organization will be notified
 - Diagnotes will evaluate whether additional users or the entire customer account should be suspended
 - Diagnotes will cooperate fully with the requesting authority and any subsequent investigation
 5. **Documentation:** All traceback requests and responses are documented and retained for compliance and audit purposes.
-

7. TERMS OF USE

Diagnotes maintains end user terms of use ("TOU") and other binding terms in its services agreements that customers must agree to before being permitted to use Diagnotes' software. Among other things, the TOU and other binding terms prohibit the use of Diagnotes products and services for purposes other than "to communicate in the facilitation of a healthcare activity such as treatment, payment, or healthcare operations."

8. CONTACT INFORMATION

For traceback requests, robocall-related inquiries, or compliance matters:

Primary Contact:

Name: Andrew Kurtz

Title: Senior Principal Engineer

Email: backlinevendors@drfirst.com

Phone: 317.263.4626

Diagnotes commits to responding to traceback requests within 24 hours.

9. COMMITMENT TO COMPLIANCE

Diagnotes is committed to preventing illegal robocall traffic and maintaining compliance with FCC regulations. We continuously monitor our systems for abuse, maintain comprehensive logging for accountability, and can take immediate action to suspend bad actors.

Our voice services serve a legitimate healthcare purpose — enabling providers to communicate with patients while protecting provider privacy — and we have implemented multiple layers of controls to ensure these services are not misused for illegal calling activity.

We will continue to review and enhance our robocall mitigation practices as FCC requirements evolve and as new best practices emerge in the industry.

End of Robocall Mitigation Plan