
Date: March/31/2026

Robocall Mitigation Plan

1. Provider Information

- **Business Name(s):** A New Vision in Educational Services & Materials Inc. (NEVESEM) d.b.a DREYFOUS
- **Primary Address:** PMB 641 HC-1 Box 29030, Caguas PR 00725-8900
- **Contact Person:** Alexander López-IT Manager – alopez@dreyfous.com
- **Overview:** Educational (K-12), Small Business & Enterprise Hosted PBX, Sip Trunk VOIP Service Provider & Systems Integrator.
- **STIR/SHAKEN Implementation Status:**
- **No STIR/SHAKEN Implementation** – DREYFOUS is unable to implement STIR/SHAKEN due to a lack of control over the network infrastructure necessary to implement STIR/SHAKEN (47 C.F.R. § 64.6305(d)(2)(i)). DREYFOUS voice services are fully hosted on the SkySwitch platform; DREYFOUS does not operate a signing function and does not maintain an STI certificate. STIR/SHAKEN authentication for calls originated on the SkySwitch platform is performed within SkySwitch-controlled infrastructure. DREYFOUS relies on this hosted implementation and maintains a robocall mitigation program consistent with 47 CFR § 64.6305.

We commit to implementing reasonable steps to avoid originating illegal robocall traffic and to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium. We will cooperate with these entities in investigating and stopping any illegal robocallers that use our service to originate calls.

3. Know Your Customer (KYC) Procedures

- **Subscriber Identification:** We use risk-based customer onboarding and account oversight designed to reduce the likelihood that customers use the services to originate illegal calls. At onboarding, and as needed thereafter, we collect and verify business identity and authority information as appropriate, which may include legal name/DBA, EIN and/or formation documentation, service address, authorized representative, contact information, and payment method. Prior to enabling outbound calling, or enabling increases in calling capability, we collect the stated use case and expected calling profile and reviews the request for consistency and reasonableness.
- **Upstream Provider Verification:** DREYFOUS does not accept third-party traffic for transit. Outbound calls originate only from DREYFOUS' end users; inbound calls are received from carrier partner(s) only for delivery to those end users. DREYFOUS coordinates with its upstream carrier partner(s) on suspected illegal traffic and traceback requests.

4. Monitoring and Detection Systems

- **Fraud Detection Services:** We use SkySwitch reporting tools, including access to call detail records and platform diagnostics, to review outbound calling activity for indicators of misuse. We investigate issues identified through platform reporting, customer complaints, upstream notifications, or traceback requests. If suspicious or illegal traffic is detected, mitigation actions may include customer outreach, warnings and remediation requests, requests for supporting documentation, temporary rate limits or blocks, including by caller ID, suspension of service, and termination for repeated or confirmed abuse.

5. Investigation and Enforcement

- **Suspension of Accounts:** Accounts engaged in suspicious activities are promptly suspended pending investigation.
- **Investigation Procedures:** Upon detecting suspicious activity, we investigate call detail records and payment information.
- **Account Suspension:** Accounts found to be engaged in illegal robocalling are suspended until a legitimate use case is provided.
- **Account Termination:** If no legitimate use case is provided, the account is terminated.

6. Traceback and Cooperation

- **Traceback Commitment:** We commit to responding fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium.
- **Cooperation with Investigations:** We will cooperate with these entities in investigating and stopping any illegal robocallers that use our service to carry or process calls.
- **Certification:** We certify that all calls originating on our network are subject to a robocall mitigation program consistent with FCC regulations.
- **Documentation:** We maintain records of our mitigation efforts and are prepared to provide documentation upon request.
- **Updates:** We will update this plan as necessary to comply with FCC requirements and to address emerging threats.