

Robocall Mitigation Plan

Nagence, Inc.

Version: May 2025

1. Company Information

- **Company Name:** Nagence, Inc.
 - **FCC Registration Number (FRN):** 0036960532
 - **Contact Information:**
 - Name: Carlos Ruiz-Diaz
 - Phone: (713) 715-7533
 - Email: legal@nagence.com
 - Address: 3200 Wilcrest Drive, Suite 170 #248, Houston, TX 77042
-

2. Description of Robocall Mitigation Program

As required by 47 CFR § 64.6305(d)(2)(ii), Nagence, Inc. has implemented a robocall mitigation program designed to prevent the origination of illegal robocalls on its network. The following outlines the specific measures employed:

a. Signup acceptance policy

- Users creating accounts using VPNs are flagged and are not allowed to make or receive calls during the trial.
- Disposable email addresses are blocked.
- We keep a list of blacklisted domains that trigger an autoban when any user tries to sign up using it.
- Non-business email users, like Yahoo or Gmail, are allowed but flagged for further screening.

b. Call Analytics and Monitoring

- The system will block any call termination to special numbers or with patterns that indicate automated means for dialing.
- The system will look for patterns showing rapid dialing to multiple destinations that are incompatible with human natural capacities.

- Regular reviews of call detail records (CDRs) to identify high-volume short-duration calls or other patterns associated with robocalling.

c. Know Your Customer (KYC) Procedures

- Signups are scored based on a series of variables, including domain used, type of IP address used (residential, proxy, VPN, etc.), country of origin.
- Our payment provider, Stripe, automatically blocks payment attempts that are compatible with known fraudulent behaviour or are part of a blacklisted set of cards reported as stolen.
- Once Stripe blocks a payment, we are notified and automatically block the account and stop all traffic until a human can review the action.

d. Blocking and Termination

- We will immediately block calls determined to be highly likely illegal robocalls.
- We will suspend or terminate the service to customers found to originate unlawful traffic.

e. Upstream provider compliance

- All of our upstream providers are in compliance, and we actively monitor that they remain as such.

List of providers:

IDT Telecom, Inc.

520 Broad Street 4th Floor, Newark, NJ 07102

Anthony Davidson

Anthony.Davidson@idt.net

Twilio Inc.

101 Spear Street, 5th Floor, San Francisco, CA 94105

Evan Finn Purtill

support@twilio.com

DIDWW Ireland Limited

10/13 Thomas Street The Digital Hub Dublin, Ireland

Ligita Chochlova

legal@didww.com

e. Complaint Intake and Response

- We maintain a dedicated communication channel (email) to receive robocall complaints from consumers, partners, and enforcement agencies.
 - We will investigate all complaints and take corrective action, including customer termination where necessary.
-

3. Certification of Commitment to Cooperate with Law Enforcement and Industry Partners

Pursuant to 47 CFR § 64.6305(d)(2)(iii), Nagence, Inc. hereby certifies that:

- It will **fully cooperate** with the FCC, law enforcement agencies, and the Industry Traceback Group (ITG) in investigations related to suspected illegal robocalls.
 - It **actively participates in traceback requests** initiated by the ITG or the FCC, responding promptly and providing necessary information to trace back the source of suspicious calls.
 - It **does not impede traceback efforts** and works in good faith to identify and eliminate the origination of unlawful robocalls on its network.
-

4. Ongoing Compliance and Updates

- Nagence, Inc. reviews its robocall mitigation practices **at least annually**, or more frequently as needed, to adapt to evolving threats and regulatory requirements.
 - Any significant changes to the mitigation program will be updated in the Robocall Mitigation Database (RMD) maintained by the FCC.
-