



Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

June 14, 2025

VIA ECFS

REQUEST FOR CONFIDENTIAL TREATMENT

Ms. Marlene H. Dortch

Secretary

Federal Communications Commission

45 L Street, NE

Washington, DC 20554

Re: Request for Confidential Treatment for Genesys Telecom US, Inc.

(FRN: 0024758419)

Call Authentication Trust Anchor, WC Docket No. 17-97

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 0.459 and in accordance with the *Sixth Caller ID Authentication Report and Order*,¹ Genesys Telecom US, Inc. (“Genesys” or the “Company”) respectfully requests that the FCC withhold from public inspection, and grant confidential treatment to, portions of Genesys’s Robocall Mitigation Plan (“Plan”) marked as confidential (Confidential Information).² The Plan, which Genesys is submitting for inclusion in the FCC’s Robocall Mitigation Database, includes proprietary and confidential business information that the Company does not make available for public inspection. Pursuant to Section 552(b) of the Freedom of Information Act (FOIA)³ and Sections 0.457 and 0.459 of the FCC’s rules,⁴ such information should be withheld from public inspection.

In accordance with Section 0.459 of the FCC’s rules, Genesys supports its request as follows:

¹ *Call Authentication Trust Anchor*, Report and Order and Notice of Proposed Rulemaking, 38 FCC Rcd 2573, ¶ 49 (2023) (“*Sixth Caller ID Authentication Report and Order*”).

² Confidential Information is denoted with: {[]}.

³ 5 U.S.C. § 552(b).

⁴ 47 C.F.R. §§ 0.457, 0.459.

(1) Identification of the specific information for which confidential treatment is sought:

Genesys seeks confidential treatment for detailed and sensitive information about Genesys's leadership.

(2) Identification of the Commission proceeding in which the information was submitted or a description of the circumstances giving rise to the submission:

Genesys is submitting the Plan in connection with the FCC's Robocall Mitigation Database requirements and related rules in 47 CFR § 64.6305. The FCC requires filers "to provide information regarding their principals, affiliates, subsidiaries, and parent companies."⁵

(3) Explanation of the degree to which the information is commercial or financial, or contains a trade secret or is privileged:

The Plan contains sensitive commercial information about the Company's leadership.

(4) Explanation of the degree to which the information concerns a service that is subject to competition:

Genesys competes for subscribers in the highly competitive voice communications industry. The Confidential Information describes the Company's business and operational details.

⁵ *Sixth Caller ID Authentication Report and Order* at ¶ 46.

(5) Explanation of how disclosure of the information could result in substantial competitive harm:

Disclosure of the Confidential Information would have a substantial adverse impact on Genesys by making available sensitive details of the Company's operations, which could be used to Genesys's detriment by its competitors.

(6) Identification of any measures taken by the submitting party to prevent unauthorized disclosure:

Genesys does not publicly disclose the Confidential Information in the normal course of business.

(7) Identification of whether the information is available to the public and the extent of any previous disclosure of the information to third parties:

Certain aspects of the Confidential Information are available for public viewing on the Company's website and other corporate disclosures. The Company does not make the Confidential Information in this format available to the public or third parties.

(8) Justification of the period during which the submitting party asserts that the material should not be available for public disclosure:

Genesys requests permanent confidential treatment and non-disclosure because it cannot identify a date certain on when the information could be disclosed without causing competitive harm.

For the foregoing reasons, Genesys submits that good cause exists to grant this request for confidential treatment. To the extent that the FCC denies this request, Genesys requests that the

enclosed materials be returned to it without consideration, pursuant to Section 0.459(e) of the FCC's Rules.⁶

Enclosed is a redacted copy of the Plan. Please direct any questions or inquiries regarding this matter to the undersigned.

Respectfully submitted,

/s/ Katy J. Milner

Katy J. Milner

Partner

Hogan Lovells US LLP

555 Thirteenth Street, NW

Washington, D.C. 20004-1109

+1 202 637 6432

⁶ 47 C.F.R. § 0.459(e).

katy.milner@hoganlovells.com

Counsel to Genesys Telecom US, Inc.

1302 El Camino Real, Suite 300

Menlo Park, CA 94025

Robocall Mitigation Plan Update 2025

Version 3.0

Contents

Overview	10
Verification of Customers	11
Monitoring Outbound Traffic.....	12
Suspicious Traffic Alerts and Tracing	13
Resources to Respond to Traceback Requests	14
Contractual Requirements.....	15
Call Signing.....	16
Call Blocking/Blacklisting.....	17
Communication with States Attorneys General.....	18
Additional Information.....	19
Summary.....	20
Attachment A.....	21

Overview

This document describes the steps Genesys has taken to avoid the origination, carrying, or processing of illegal robocall traffic.

Genesys is uniquely positioned to ensure that illegal calling (robocalling) does not occur on our network. Genesys customers utilize the platform primarily for answering inbound calls to contact centers. In addition, Genesys only provides telecommunications services to customers who purchase Genesys Cloud CX™ software subscriptions. We have accurate data on these customers including their verified company name, tax information, location, and contacts. We also have full access to and control of our customer's Genesys platform which ensures that if any illegal robocalling occurs, we can disable their trunks and/or completely revoke access to the platform. Genesys signs our customer calls for STIR/SHAKEN and no longer relies on carrier partners for call signing.

Verification of Customers

Genesys takes affirmative, effective measures to prevent new and renewing customers from originating illegal calls. Every Genesys customer is subject to vetting upon signing an agreement to purchase our platform. This includes the verification of the validity of the business entity making the purchase. (See also “Contractual Requirements.”)

Monitoring Outbound Traffic

Genesys has “know-your-upstream provider” procedures in place designed to mitigate illegal robocalls. Genesys and its upstream providers have agreed to work together diligently to mitigate all illegal robocalls, including cooperating fully when receiving traceback requests. Genesys’s master service agreement with its upstream provider contains provisions regarding robocall mitigation, i.e., that the carrier abides by all the FCC’s robocall mitigation rules.

Genesys and its partners also use proprietary advanced call analytics systems to identify and block illegal traffic. Specifically, Genesys and its carrier partners monitor call traffic for suspicious patterns, such as spikes in traffic to unexpected destinations or anomalies in recent call volumes generated by calls from a single customer compared to weekly trends. We track and analyze calling and connectivity data for unusual patterns, which generate alerts to indicate the need for further investigation by operations personnel. Our carrier partners notify Genesys of any potential fraud or illegal calling. Genesys teams are then able to investigate and take appropriate actions to block or allow these calls.

Genesys does not use any third-party analytics vendors to identify and block illegal traffic.

Suspicious Traffic Alerts and Tracing

Genesys can trace every call that occurs on our network back to specific customers and/or individual users of our platform. This capability is based on extensive logging of user logins, originating IP address of those logins, and call detail records. In addition, Genesys telecommunications operations personnel receive alerts when suspicious traffic patterns are detected on our carrier partner networks.

Resources to Respond to Traceback Requests

Genesys has a team of telecommunications management personnel who operate and maintain our telecommunications services. Genesys telecommunications operations team is prepared to respond to traceback requests at any time that they are requested, and is committed to responding within 24 hours to all traceback requests from the FCC, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to carry or process calls.

Contractual Requirements

Genesys contractually obligates all customers to comply with all legal and regulatory requirements including outbound telemarketing legislation. Specifically, our “Compliance with Laws” clause of the general terms of our customer agreements includes the following:

“10.4 Compliance with Laws. Each party will comply with laws, statutes, rules, regulations, ordinances, and other pronouncements having the effect of law (collectively “Laws”) as applicable to a party and, in the case of Customer, applicable to the Materials and their use. In no event will We be responsible for providing, implementing, configuring or coding the Materials in a manner that complies with any Laws that apply to Your business or industry, including without limitation, the Communications Act of 2003 as implemented by OFCOM, the Australia Telecommunications Act 1997 (Cth) and Acts related to telecommunications and the relevant industry codes approved by the Australian Communications and Media Authority, the UK Anti-Bribery Act, the Foreign Corrupt Practices Act, the FTC or FCC regulations or the Telephone Consumer Protection Act of 1991 (collectively “Customer Specific Laws”). You will comply with Customer Specific Laws, and in no event will We or Our business partners, licensors or suppliers be liable for any claim or action arising from or related to Your failure to comply with any Customer Specific Laws, it being understood that You are solely liable for any such failure(s) and resulting claims or actions.”

Call Signing

Genesys has fully implemented STIR/SHAKEN for call signing. Genesys has obtained an OCN and has partnered with STIR/SHAKEN call signing technology providers to sign all calls originated on our platform. Customers may also decide to pursue centralized number registration databases through our partners as part of their overall solution.

Call Blocking/Blacklisting

Genesys can block any incoming traffic by blacklisting telephone numbers upon request.

Communication with States Attorneys General

Genesys legal and telecommunications management teams cooperate with States Attorneys General regarding recognized scams and illegal robocalling.

Additional Information

- **Corporate Information:**
 - Parents and Owners: Genesys Telecom US, Inc. is a wholly owned subsidiary of Genesys Cloud Services, Inc. Through a series of intermediate holding companies, Genesys Cloud Services, Inc. is ultimately privately owned by investors and funds.
 - Subsidiaries and Affiliates: Genesys Telecom US, Inc. has no subsidiaries and no affiliates that provide services to the public.
 - Directors, Officers, and Principals: A table of the Genesys officers and directors is included as Attachment A. Genesys's leadership team and its Board of Managers are listed on its website at <https://www.genesys.com/company/leadership>.
 - Principals: Apart from the entities and individuals listed above, Genesys has no other principals who exercise management or control of Genesys.
- **OCN:** Genesys Telecom US, Inc.'s OCN is 393K.
- **Services:** Genesys Telecom US, Inc. provides DID and toll-free telephone numbers as well as inbound and outbound calling services to business customers who purchase a Genesys Cloud software subscription. We do not sell services to non-Genesys Cloud customers.
- **Actions and Investigations:** In the past 2 years, neither Genesys nor any entity for which Genesys shares common ownership, management, directors, or control has been the subject of a formal FCC, law enforcement, or regulatory agency action or investigation pertaining to the transmitting, encouraging, assisting, or otherwise facilitating of illegal robocalls or spoofing or a deficient Robocall Mitigation Database certification or mitigation program description.
- **Traceback Requests:** Genesys has, to date, received only 2 traceback requests, which it has responded to, and which was determined not to be fraudulent, but legitimate calling activity. We have, separately, received several reports of inbound caller-id spoofing coming from other carriers.
- **Call Chain:** Genesys is a voice service provider with a STIR/SHAKEN implementation obligation serving end-users. Genesys has fully implemented STIR/SHAKEN for call signing.

Summary

Genesys has a low risk of illegal robocalling occurring on our network because we only sell telecommunications services to customers who are utilizing our platform whom we vet as part of the sales process. Genesys has taken all reasonable measures to ensure that robocalling does not occur on our network, to monitor the network for suspicious calling patterns, and to ensure that the resources are available to work with our partners and the FCC to investigate and perform traceback requests. Genesys is now signing calls for STIR/SHAKEN compliance.

Contact:

Christopher W. Jones
Senior Director, Commercial Telco Mgmt, Genesys Cloud
10350 Longmont Dr.
Houston, TX 77042
Ph: (832) 316-0383
Chris.Jones@genesys.com

Attachment A

REDACTED