

Robocall Mitigation Program Description

1. Company Information

Company Name: GLOBALCONNECT A/S

Contact Person: Mikkel Sylvest

Email: mikkel.sylvest@globalconnect.dk

Phone: +45-40993016

Address: Havneholmen 6, st., 2450 København SV

VAT Number: DK26759722

2. STIR/SHAKEN Implementation

Exemption Statement: Per FCC regulations under **47 CFR § 64.6304(a)**, providers that do not have direct interconnection with the public switched telephone network (PSTN) in the United States are not required to implement the STIR/SHAKEN authentication framework.

GlobalConnect A/S is a European-based provider that transmits traffic to the United States via wholesale carrier agreements. As such, GlobalConnect does not have direct interconnection with the U.S. PSTN. Traffic is handed off to upstream carriers who are responsible for STIR/SHAKEN compliance within the U.S. network. GlobalConnect, however, implements a robust robocall mitigation program to monitor and prevent fraudulent traffic in compliance with **47 CFR § 64.6305(a)**. Our company has selected the following certification level, Option 3.

-

We certify that all of the calls that we originate on our network are subject to a robocall mitigation program consistent with 47 CFR § 64.6305(a), which includes reasonable steps to avoid originating illegal robocall traffic. We commit to responding fully and within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use our service to originate calls. We also certify that any prior certification has not been removed by Commission action, that we have not been prohibited from filing in the Robocall Mitigation Database by the Commission, and that we have not implemented the STIR/SHAKEN authentication framework on any portion of our network.

3. Robocall Mitigation Strategy Our company has implemented the following measures to prevent illegal robocalls:

- **Know Your Customer (KYC):** We conduct due diligence on new customers, verifying business legitimacy before granting service.

- **Traffic Monitoring:** We analyze call traffic patterns through our Cisco Broadsoft platform for irregularities indicative of potential robocall activity.
- **Call Blocking and Filtering:** We allow only specific traffic from known customers connected to our platform. 90% of our customers are end-users, where we have a KYC process and a termination agreement with the customer.
- **Wholesale Traffic Control:** The remaining traffic consists of wholesale segment traffic, which passes through our Cisco Broadsoft platform, where we analyze and route traffic.
- **Regular Traffic Analysis:** We monitor and analyze our traffic frequently (**no less than hourly**) and take appropriate actions, such as updating routing and/or blocking destinations or originating numbers when necessary.
- **Collaboration with Authorities:** We respond to traceback requests from the FCC, law enforcement, and the industry traceback consortium within 24 hours.

4. Network Description Our network consists of:

-

Our call processing is managed through a combination of Cisco Broadsoft and Ribbon platforms, allowing us to monitor and control all traffic using CDR data, which is processed every 15 minutes. While STIR/SHAKEN has not yet been implemented, we maintain strict monitoring and mitigation practices to ensure compliance with regulatory requirements. We are in dialogue with Cisco regarding the implementation of STIR/SHAKEN for the relevant portions of our platform and traffic.

5. Procedure for Handling Suspected Robocalls

- Suspicious traffic is flagged using automated alerts, and our operations team conducts evaluations to determine necessary actions, such as blocking or rerouting calls. Blocking actions, if necessary, are handled manually by our security-cleared staff, who operate 24/7.
- We investigate any reported suspicious traffic and take appropriate action, including blocking or terminating services for customers found to be engaging in illegal robocall practices.
- We maintain escalation procedures for handling violations, ensuring compliance with FCC regulations.

6. Compliance Commitment We certify that our robocall mitigation efforts align with the requirements of 47 CFR § 64.6305 and that we actively work to prevent the origination of illegal robocalls on our network.

Confidentiality Request (If Applicable) Our company requests confidentiality for specific aspects of this filing in accordance with the Electronic Comment Filing System (ECFS). If applicable, a formal request has been submitted separately.

Authorized Representative: Name: Mikkel Sylvest
Title: Senior Manager, Head of Delivery & Billing
Date: February 25th, 2025