

Robocall Mitigation Plan – Europeer Limited

Version - Partial STIR/SHAKEN Implementation

1. Introduction - Type of Provider Filing

Europeer Limited is a Voice Service Provider Filing and Non-Gateway Intermediate Provider Filing. Is a foreign entity incorporated in Hong Kong, with operational and commercial activities conducted internationally. Network routing and compliance controls applicable to U.S. traffic are centrally managed in accordance with the below described Robocall Mitigation Plan.

2. Partial STIR/SHAKEN Implementation

Europeer Limited is subject to the Partial STIR/SHAKEN Implementation because is a foreign, Hong Kong company operating outside the United States, with a network infrastructure that is only partially subject to U.S. STIR/SHAKEN implementation requirements.

At this stage, full end-to-end STIR/SHAKEN deployment across our network is not technically feasible due to differences in international regulatory frameworks, network architecture, and interconnection with foreign carriers. Depending on the specific service configuration, Europeer Limited may act as an originating provider, transit provider, or intermediate provider for voice traffic involving the United States. The robocall mitigation measures described in this Plan are applied consistently with Europeer Limited's role in the call path and in accordance with applicable FCC requirements.

Therefore, Europeer Limited has implemented the STIR/SHAKEN authentication framework on the portion of the network, related to the United States traffic, where it is technically and operationally possible, and all calls originated on that portion of the network are fully compliant with 47 CFR § 64.6301(a)(1) and (2).

3. STIR/SHAKEN Attestation Decision Framework

Europeer Limited does not originate STIR/SHAKEN signatures on voice traffic. Where STIR/SHAKEN authentication is required for U.S.-bound traffic, Europeer Limited relies on authorized upstream or downstream interconnect partners to perform call signing. Europeer Limited's network securely passes authenticated calls without modification.

Attestation requests are made based on the following operational criteria:

- **Attestation A (Full Attestation):**

Requested when the calling number (DID) is assigned by the interconnect partner and full end-user number ownership and authorization have been verified through documented proof of number assignment and customer identity.

- **Attestation B (Partial Attestation):**

Requested when there is a direct contractual relationship with the customer and verifiable authorization to use the calling number exists, but full end-user number ownership cannot be independently established.

- **Attestation C (Gateway Attestation):**

Europeer Limited does not request, apply, or require Attestation C for any traffic.

Where STIR/SHAKEN signing cannot be applied by an interconnect partner for U.S.-bound traffic, Europeer Limited applies role-appropriate robocall mitigation measures and may restrict, suspend, or reject traffic based on interconnect requirements, regulatory obligations, or risk assessment.

4. STIR/SHAKEN Authentication processes

Where STIR/SHAKEN authentication is required for U.S.-bound traffic, Europeer Limited may rely on upstream or downstream interconnect partners to perform call signing. In such cases, Europeer Limited's network infrastructure is capable of securely passing authenticated calls without modification and does not interfere with valid STIR/SHAKEN signatures.

When numbering resources (DIDs) are obtained from an interconnect partner, Europeer Limited requests appropriate STIR/SHAKEN attestation consistent with the level of customer and number authorization available. Specifically, calls may be signed with **Attestation A** where full end-user and number ownership is established, or **Attestation B** where there is a direct customer relationship and verifiable authorization to use the calling number. Europeer Limited does not require or request signing of calls with **Attestation C**.

When Europeer Limited functions as an originating provider, robocall mitigation measures include customer onboarding and KYC verification, review of intended calling use cases, monitoring for unlawful or abusive calling patterns, and enforcement actions including traffic restriction, suspension, or termination for non-compliant activity.

Europeer Limited retains call detail records and keeps logs for a minimum of 12 months, or longer where required to support traceback investigations or regulatory requests.

For traffic originated outside the United States and transiting international networks, STIR/SHAKEN signing may not be technically applicable or required at the point of origination under current regulatory and technical frameworks. In such cases, Europeer Limited applies robocall mitigation measures appropriate to its role in the call path and complies with applicable FCC requirements for non-U.S. originating traffic terminating in the United States.

5. Robocall Mitigation Internal Procedure

In parallel, Europeer maintains a robust robocall mitigation program that applies to all calls originated on our network, in full compliance with 47 CFR § 64.6305(a). This program includes reasonable and effective measures to prevent the origination of illegal robocall traffic, continuous monitoring of call activity, and strict internal controls.

Our robocall mitigation program includes, but is not limited to:

- Customer due diligence and KYC procedures prior to service activation;
- Ongoing traffic monitoring for abnormal call volumes, short-duration calls, and invalid or unassigned calling numbers;
- Traffic monitoring and enforcement measures include analysis of calling numbers (A-numbers), including detection of invalid, spoofed, or high-risk number patterns. Europeer Limited may suspend, restrict, or terminate traffic associated with calling numbers involved in illegal or suspicious robocall activity.
- Immediate suspension or termination of customers generating illegal robocall traffic;
- Automated detection of traffic anomalies such as sudden volume spikes, low average call duration (ACD), and abnormal answer-seizure ratios (ASR).
- Maintenance of call records and logs sufficient to support traceback requests.

6. Cooperation with U.S. authorities

As a foreign company providing services that may terminate in the United States, we are committed to full cooperation with U.S. authorities and industry partners. We certify our commitment to:

- Respond fully and within 24 hours to all traceback requests from the FCC, law enforcement agencies, and the industry traceback consortium;
- Cooperate in investigations and take prompt action to stop any illegal robocall traffic using our services.

Conclusion

By selecting Partial STIR/SHAKEN Implementation, our company demonstrates both regulatory compliance and good-faith efforts to align with U.S. anti-robocall requirements while operating within the technical and legal constraints applicable to an international carrier.