Zernikepark 12, 9747 AN Groningen, Netherlands · KvK 89748468 · VAT NL865089978B01

Robocall mitigation contact: James Seo, Director, compliance@zylon-voip.nl, +31 50 3604554

Robocall Mitigation Program Description

Field	Value
Filing Entity	Zylon Internet B.V.
Brand / DBA	zylon-voip.nl
Address	Zernikepark 12, 9747 AN Groningen, Netherlands
Telephone	+31 50 3604554
VAT	NL865089978B01
KvK (Chamber of Commerce)	89748468
Filing Type	Voice Service Provider (foreign voice service provider)
Applicable Rule	47 CFR § 64.6305(d)(2)(i)–(iii)

1. Introduction and Certification Scope

Zylon Internet B.V. ("Zylon"), a limited liability company organized under the laws of the Netherlands and registered with the Dutch Chamber of Commerce (KvK) under number 89748468, is a **foreign voice service provider** within the meaning of 47 CFR § 64.6300(c). Zylon provides outbound voice service from its own telecommunications facilities located in the Netherlands, and has the ability to originate voice service that terminates in the United States. Zylon therefore files this robocall mitigation program description in the Federal Communications Commission's Robocall Mitigation Database as required by 47 CFR § 64.6305(d).

This document is submitted in satisfaction of 47 CFR § 64.6305(d)(2)(i), (ii) and (iii). It describes (i) the basis for Zylon's certification level with respect to the STIR/SHAKEN caller ID authentication framework, (ii) the specific reasonable steps Zylon has taken to avoid originating illegal robocall traffic, and (iii) Zylon's commitment to respond to traceback requests.

Zylon originates outbound calling campaigns on its own FreeSWITCH 1.10 infrastructure running on Debian, hosted on hardware located in the Netherlands. Zylon holds dedicated SIP trunks to United States and international carriers and allocates a dedicated DID pool to each customer. Zylon serves business customers such as contact centres, lead generation firms, and collections operations. Zylon does not operate as a gateway provider or as an intermediate provider; it originates traffic directly and delivers it to end users.

This document is provided in English, as required by 47 CFR § 64.6305(d)(2). No request for confidential treatment of the contents of this document has been made under 47 CFR § 0.459.

2. Part (d)(2)(i) — Certification Basis and STIR/SHAKEN Status

2.1 Basis for the certification level selected

Zylon certifies under **Option 2 — Partial STIR/SHAKEN Implementation**.

Zylon originates outbound voice traffic on a network that combines IP-based and non-IP-based components. Specifically:

- Zylon's origination platform is IP-based. Traffic is generated by our FreeSWITCH 1.10 softswitch on Debian, and the customer-facing leg is delivered as SIP over IP. Because Zylon originates calls on an IP-based network, Zylon's originated calls are within the scope of 47 CFR § 64.6301(a) and (b).
- Zylon originates calls to United States destinations using NANP numbers in the caller ID field, and delivers those calls over a fixed SIP trunk to its United States carrier. Zylon does not control the end-to-end carrier network beyond the trunk handoff, and therefore does not control the full signalling path for every call it originates.

2.2 Why a full (Option 1) certification is not made

Zylon does not certify full STIR/SHAKEN implementation across its entire network for two concrete reasons:

1. **Portion of the network is non-IP.** A portion of the call path for calls Zylon originates terminates in carrier infrastructure that is not IP-based for the signalling exchange with the receiving party. Under the Commission's guidance, Option 1 is not appropriate where a portion of a provider's network is non-IP, even if STIR/SHAKEN has been fully implemented on the IP portion. In this circumstance the provider must select Option 2 — Partial STIR/SHAKEN Implementation.
2. **Limited control over downstream network infrastructure.** Zylon's control over the network infrastructure necessary to implement STIR/SHAKEN is limited to its own origination platform and the immediate trunk handoff to its carrier. Zylon does not control the numbering resources, the access network, or the switching and transport infrastructure of the carriers and exchanges that deliver calls to the called party.

2.3 Scope of implementation on the IP portion of the network

On the IP-based portion of Zylon's network:

- United States numbers originating on Zylon's platform are signed with **STIR/SHAKEN A-level (full attestation)** where the carrier path supports it, and with the appropriate lower attestation level where the downstream path does not support full attestation. Zylon's compliance page describes this arrangement: United States numbers are signed with STIR/SHAKEN A-level attestation via the carrier and are registered with freecallerregistry.com and the FCC Robocall Mitigation Database.
- Zylon maintains a **dedicated DID pool per customer**, with CNAM records configured for each customer and STIR/SHAKEN attestation applied per customer. Each customer's outbound campaign therefore runs on caller ID that is bound to that customer, which is what makes traceback possible in the first place.
- Zylon is registered with the **STIR/SHAKEN Policy Administrator** and has obtained its own SPC token, which it uses to generate certificates with a Certificate Authority to authenticate calls it originates, as required for a provider certifying to partial STIR/SHAKEN implementation.
- All calls Zylon originates on the IP portion of its network are authenticated in accordance with 47 CFR § 64.6301(a) and (b) to the extent the downstream carrier path supports authentication.

2.4 Explanation of why STIR/SHAKEN cannot be fully implemented

Zylon is unable to implement the STIR/SHAKEN authentication framework across its entire network because it lacks control over the network infrastructure necessary to do so. Zylon is a originating voice service provider operating from a single country of origin, the Netherlands, and it does not operate the access, transport, or switching infrastructure in the United States through which its traffic is delivered. Zylon can only control the

signalling it generates on its own platform and the signalling exchanged with its immediate trunk provider. Calls that traverse non-IP segments of the downstream path cannot be authenticated end-to-end by Zylon.

---

3. Part (d)(2)(ii) — Reasonable Steps to Avoid Originating Illegal Robocall Traffic

3.1 Compliance with the obligation to know its customers (47 CFR § 64.1200(n)(4))

Zylon satisfies its obligation to know its customers under 47 CFR § 64.1200(n)(4) before accepting traffic and before enabling a customer to originate calls. The following procedures are applied:

- **Documented customer identification.** Zylon enters into a written agreement with each customer that identifies the legal entity, the registration number, the business address, and the individuals responsible for the customer's outbound campaigns. Commercial terms are accepted only after the customer's legal identity has been verified against the Dutch Chamber of Commerce register or an equivalent official register.
- **Ongoing verification.** The customer record is re-verified at the time of each contract renewal and whenever the customer is onboarded to a new trunk or a new DID pool.
- **Named individual accountability.** Each customer account is bound to a specific contactable customer and a specific set of customer administrators. Zylon does not sell or resell carrier service anonymously.
- **Suspension and termination.** Accounts that fail identity verification, that fail repeated anti-fraud screening, or that are the subject of a substantiated abuse report are suspended immediately and terminated where the abuse is severe or recurring.
- **Complaint handling.** Zylon operates a published complaints procedure at `https://zylon-voip.nl/klacht/`. Complaints are logged, investigated, and fed back into the anti-fraud screening rules described below.

3.2 Procedures to know upstream providers

Zylon's upstream providers are known and documented as follows:

- **Fixed SIP trunk to a United States carrier.** Zylon's primary United States carrier is BulkVS. The trunk is provisioned with **IP authentication**: the softswitch presents a static, whitelisted source IP address, and the carrier only accepts traffic from those addresses. Trunk credentials are not shared with customers and cannot be used to originate traffic directly.
- **International trunk.** Zylon's international carrier is DIDWW, likewise connected over IP-authenticated SIP.
- **Provider due diligence.** Before a carrier is onboarded, Zylon reviews the carrier's regulatory status, its own anti-fraud and traffic-management posture, and its identity registration with the relevant national numbering and regulator authorities. The carrier relationship, the trunk endpoints, and the IP authentication configuration are recorded in Zylon's internal carrier register.
- **No resold, unverified upstream transit.** Zylon does not accept traffic from an upstream provider that it has not itself contracted, verified, and connected on IP-authenticated infrastructure. There is no open or anonymous SIP peering.
- **Upstream traffic restrictions.** The US trunk is configured to originate only to destinations allocated to NANP resources. Zylon does not permit the trunk to be used to originate traffic to any destination outside the United States, which constrains the upstream path to a single, identifiable numbering plan.

3.3 Analytics system(s) used to identify and block illegal traffic

Zylon operates a **self-hosted analytics and enforcement stack built on its own FreeSWITCH 1.10 signalling and media platform**. Zylon does **not** use any third-party analytics vendor for the purpose of identifying or blocking illegal robocall traffic, and does not disclose any third-party analytics vendor name, because none is used. The analytics functions described in this section are performed entirely in-house.

The self-hosted stack performs the following functions:

- **Real-time signalling analytics.** FreeSWITCH's SIP event logging captures, for every call, the originating customer, the originating IP and trunk, the caller ID and the called number in E.164 form, the campaign and dialer identifier, the call start time, the call duration, and the disposition of the call. These records are retained and queryable for the full retention period stated in Section 3.6.
- **Concurrent-call and pacing analysis.** The stack computes per-customer and per-campaign call concurrency, calls-per-second, and hourly volume, and compares each against the profile established for that customer. Sustained deviation from the agreed profile is treated as a fraud or robocall signal.
- **Duration and answer-rate analysis.** The stack identifies campaigns with implausibly short or uniform call durations, low answer rates, and high hang-up rates, which are characteristic of automated or deceptive dialing.
- **Repetitive-content detection.** Where a campaign uses prerecorded or synthesized audio, the stack analyses call duration distributions and repeat-pattern metrics to distinguish legitimate agent-handled contact from automated dialing.
- **Caller ID and numbering analysis.** The stack checks that the caller ID presented on each call belongs to the customer and DID pool that originated it, detects caller ID values that are not provisioned to the originating customer, and detects reuse of a caller ID across customers. Spoofed or mismatched caller IDs are blocked at origination.
- **Known-illegal-number and blocklist enforcement.** The stack maintains Zylon's own blocklist and denylist of numbers known to originate or receive illegal robocalls, and enforces the applicable do-not-call and restricted-list regimes for the destination market before the call is placed.
- **Destination filtering and rate control.** Calls to restricted or otherwise disallowed destinations are dropped at origination. Per-destination and per-customer pacing limits are enforced in real time.
- **Traffic anomaly alerting.** Deviations from baseline volume, concurrency, geography, and duration profiles raise an alert to Zylon's abuse and operations personnel for review before the traffic can scale further.

3.4 Specific blocking and enforcement measures

The following reasonable steps are taken to avoid originating illegal robocall traffic:

1. **Customer-specific origination controls.** Each customer is provisioned with a dedicated DID pool, dedicated trunk authorization, and customer-scoped dialing permission lists. A customer cannot originate traffic from a numbering resource, destination, or trunk that has not been assigned to it.
2. **Per-campaign approval.** Outbound campaigns require registration of the campaign identifier, target list, permitted calling hours, permitted destination types, and the script or audio asset before calls are permitted. Origination is blocked until the campaign profile is approved.
3. **Calling-hour enforcement.** Calls are blocked outside 08:00–21:00 local time of the called party, in line with the calling-time restrictions Zylon applies and publishes.
4. **National and international do-not-call screening.** Originating numbers and target lists are screened against the applicable national do-not-call registry and against restricted-number regimes for the

destination market. Where a local disclosure or do-not-call regime applies to the destination market, the required announcement or recorded disclosure is played at the beginning of the message.

5. **Known-illegal-traffic blocking.** Calls to numbers on Zylon's internal blocklist and denylist are blocked at origination and are not dialed.
6. **Pacing and concurrency limits.** Enforced per customer, per campaign, per trunk, and per destination. Limits are set to the customer profile and are tightened immediately when a monitoring signal fires.
7. **Immediate suspension on signal.** Where the analytics stack raises an anomaly, the affected customer or campaign is subject to immediate suspension of origination pending investigation, and the originating platform enforces the suspension directly rather than relying on the customer to comply.
8. **Emergency-call protection.** Zylon does not block, rate-limit, or otherwise interfere with any call to 911 or to any government emergency number or public safety answering point. Emergency calls are given priority and are exempt from all blocking and pacing controls described in this section, consistent with 47 CFR § 64.6305(g)(5).

3.5 STIR/SHAKEN and caller ID integrity controls

- Every DID and CNAM in a customer's pool is registered to that customer and is used only for that customer's traffic.
- STIR/SHAKEN attestation is applied per DID pool, with A-level attestation used where the carrier path supports it.
- Caller ID values that are not provisioned to the originating customer are blocked at origination and flagged for investigation.
- Zylon does not permit customer-supplied caller ID values to be presented on the network except where the value is a number provisioned by Zylon to that customer.

3.6 Retention, monitoring, and review

- Origination records — signalling logs, campaign configuration, and enforcement actions — are retained for a minimum of **24 months** and are available to the FCC, U.S. law enforcement, and the industry traceback consortium on request.
- Automated anomaly detection runs continuously; automated reporting is reviewed by Zylon personnel on a daily basis, and the anti-fraud and blocking configuration is reviewed and adjusted on at least a monthly basis.
- Zylon's screening rules, blocklists, and campaign-approval criteria are reviewed at least quarterly, and are updated whenever a new enforcement notice, traceback request, or customer complaint identifies a new abuse pattern.

---

4. Part (d)(2)(iii) — Commitment to Respond to Traceback Requests

Zylon commits as follows:

1. **24-hour response commitment.** Zylon commits to respond **within 24 hours** to all traceback requests from the Commission, U.S. law enforcement, and the industry traceback consortium (the "Traceback Consortium") concerning calls that Zylon originated, and to cooperate fully with such entities in investigating and stopping any illegal robocallers that use Zylon's service to originate calls.
2. **Full cooperation.** Zylon will cooperate with the Commission, U.S. law enforcement, and the Traceback Consortium in the investigation of any illegal robocalls originating from its network, including by providing

call detail records, campaign and customer attribution, audio recordings where available and legally permissible, and information about the customer's originating platform configuration.

3. **Traceback procedure.** Upon receipt of a traceback request, Zylon's robocall mitigation point of contact will: * acknowledge receipt to the requesting authority; * search the originating signalling records for the called number and the date and time of the call, matching on the called number in E.164 form, the calling number, and the time window; * identify the originating customer and the specific DID and CNAM used; * identify the dialer or campaign configuration that placed the call and the calling IP address and trunk used; * determine whether the call originated from Zylon's platform and, if so, provide the requested subscriber information; * where the call did not originate from Zylon's platform, identify the upstream provider to which the traffic was delivered and forward the traceback request to that provider; * take immediate enforcement action, including suspension of the originating customer or campaign, where the traceback indicates illegal robocall activity; and * report the outcome of the investigation to the requesting authority.
4. **Records sufficient to complete traceback.** Zylon maintains the origination records described in Section 3.6 for a minimum of 24 months, which is sufficient to satisfy traceback requests relating to the period during which the call was originated. Zylon will retain records for a longer period where a traceback request or an investigation is pending.
5. **Single point of contact.** Traceback requests are directed to Zylon's robocall mitigation point of contact identified in the Robocall Mitigation Database filing, and are monitored continuously during Dutch business hours and, on a best-effort basis, outside those hours. Zylon acknowledges that the 24-hour commitment is measured in elapsed time and not in business hours, and Zylon's operational procedures are structured to meet an elapsed-time standard.
6. **Escalation.** Where a traceback request cannot be resolved within the 24-hour window on initial review, Zylon notifies the requesting authority within the 24-hour window with an interim status, the information identified so far, and a committed time for the complete response.

---

5. Part (d)(2)(iv) — Prior Commission or Law Enforcement Action

Zylon has not, in the prior two years, been the subject of any formal Commission, law enforcement, or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to Zylon transmitting, encouraging, assisting, or otherwise facilitating illegal robocalls or spoofing, or due to a deficient Robocall Mitigation Database certification or mitigation program description. This statement covers Zylon Internet B.V. and any entity with which Zylon shares common ownership, management, directors, or control.

---

6. Updating Filings

Zylon will update this filing within 10 business days of any change to the information required by 47 CFR § 64.6305(d)(1) through (d)(4), in accordance with 47 CFR § 64.6305(d)(5). Zylon will certify annually, on or before March 1, that the information submitted to the Robocall Mitigation Database is true and correct, as required by 47 CFR § 64.6305(h).

---

7. Declaration

Zernikepark 12, 9747 AN Groningen, Netherlands · KvK 89748468 · VAT NL865089978B01

Robocall mitigation contact: James Seo, Director, compliance@zylon-voip.nl, +31 50 3604554

I declare that the foregoing robocall mitigation program description is true, correct, and complete, and that the information submitted in connection with this certification in the Robocall Mitigation Database is true, correct, and complete.

Field	Value
Filing Entity	Zylon Internet B.V.
Business Address	Zernikepark 12, 9747 AN Groningen, Netherlands
Telephone	+31 50 3604554
Email	info@zylon-voip.nl

Signed by: James Seo — Director — November 4, 2026

`Name: _____`
`Title: _____`
`Date: _____`
Signed by an officer in conformity with 47 CFR § 1.16.