



REGULATORY COMPLIANCE — FCC ROBOCALL MITIGATION DATABASE

Robocall Mitigation Program Description

v1.0

Filed pursuant to 47 CFR § 64.6305(d) and (f) in support of RWTS's Robocall Mitigation Database certification as a foreign voice service provider

AUTHOR

Andrew Yager

DATE

July 2026

CLASSIFICATION

Public (RMD filing)

Introduction and Purpose

Real World Technology Solutions Pty Ltd (**RWTS**) submits this Robocall Mitigation Program Description in support of its certification in the Federal Communications Commission's Robocall Mitigation Database (RMD), filed under FCC Registration Number (FRN) **0038693651**.

RWTS is a **foreign voice service provider** within the meaning of 47 CFR § 64.6300(c). RWTS provides voice services from Australia and originates voice traffic that terminates to subscribers in the United States via one or more US-based gateway providers. RWTS also provides wholesale voice connectivity to other providers, and for their US-destined traffic acts as a **non-gateway intermediate provider**. RWTS accordingly files in the RMD in both capacities, pursuant to 47 CFR § 64.6305(g)(2), so that US-based intermediate providers and voice service providers may lawfully accept its traffic.

This document describes, with particularity, the reasonable steps RWTS takes to ensure it does not originate illegal robocall traffic, consistent with 47 CFR § 64.6305(d) and (f) and the guidance in the Commission's Filing Instructions Public Notice, DA 24-73. It covers RWTS's customer due diligence (know-your-customer) practices, calling line identification controls, traffic monitoring and analytics, traceback cooperation, the know-your-upstream-provider controls applied to wholesale customers, and the procedures RWTS follows when notified of suspected illegal traffic.

Corporate Information

ITEM	DETAIL
Legal name	Real World Technology Solutions Pty Ltd
Trading names	Real World Technology Solutions; Real World; HyperConnect (retail ISP brand); Lux Imperium; Red Globe Productions
ABN	74 101 234 664
FCC Registration Number	0038693651
Registered office	12/2 Eden Park Drive, Macquarie Park NSW 2113, Australia
Country	Australia
Autonomous System	AS45437

Principals, affiliates, subsidiaries and parent companies. RWTS is an Australian-owned company. Its sole director and principal is Andrew Yager, Managing Director. Lux Imperium and Red Globe Productions are trading names of RWTS, not separate legal entities. The only related entity is Real World Networks Pty Ltd, a separately licensed Australian carrier (Carrier Licence No. 387) under common ownership. Real World Networks Pty Ltd is a network-only carrier operating solely within Australia: it provides no voice services of any kind and does not originate, carry or process any voice traffic. All traffic covered by this filing is handled by RWTS.

Regulatory Status in Australia

RWTS operates as a **Carriage Service Provider (CSP)** under the Telecommunications Act 1997 (Cth) and is regulated by the Australian Communications and Media Authority (ACMA). RWTS operates its own carrier-grade IP network and voice platform; it is not a reseller of another provider's switching.

RWTS's originating conduct is already subject to a mature Australian anti-scam and anti-spam regime that parallels, and in several respects predates, the Commission's robocall mitigation framework:

- **Reducing Scam Calls and Scam SMS Industry Code (C661:2022).** A mandatory, ACMA-registered code requiring Australian providers to identify, trace, block and otherwise disrupt scam calls and scam SMS, to verify customer identity, to share scam intelligence with other providers, and to cooperate with ACMA and other providers in tracing scam traffic to its source.
- **Spam Act 2003 (Cth)** and the **Do Not Call Register Act 2006 (Cth)**, governing commercial electronic messages and telemarketing calls respectively.
- **SMS Sender ID Register.** RWTS is registered with ACMA as both a participating and certified telecommunications provider under the Telecommunications (SMS Sender ID Register) Industry Standard 2025, reflecting its existing investment in sender identity verification and anti-impersonation controls.
- **Scams Prevention Framework.** RWTS maintains compliance readiness under Australia's Scams Prevention Framework Act 2025 (Cth), including external dispute resolution arrangements.

RWTS applies the same customer verification, monitoring and enforcement disciplines described in this document to all traffic it originates, regardless of destination. Traffic destined for the United States receives no lesser scrutiny than domestic Australian traffic.

STIR/SHAKEN Implementation Status

RWTS certifies to **Option 3 – No STIR/SHAKEN Implementation** in both the "Voice Service Provider Certification" and "Non-Gateway Intermediate Provider Certification" sections of its RMD filing, reflecting the two capacities in which it handles US-destined traffic.

RWTS is unable to implement the STIR/SHAKEN authentication framework described in 47 CFR § 64.6301 because, as a foreign voice service provider with no United States operations, it is not eligible to register with the STIR/SHAKEN Policy Administrator or to obtain a Service Provider Code (SPC) token and STI certificate. Participation in the STIR/SHAKEN governance framework requires an FCC Form 499A filing, an Operating Company Number, and access to US numbering resources, none of which are available to RWTS. RWTS therefore cannot authenticate calls with its own certificate as required by 47 CFR § 64.6301 and § 64.6305(h).

Calls originated by or carried through RWTS and destined for the United States enter the US network via a US-based gateway provider, which applies caller ID authentication in accordance with its own obligations under 47 CFR § 64.6302. RWTS confirms that all calls it originates, carries or processes on its network are instead subject to the robocall mitigation program described in this document.

Know Your Customer (KYC)

RWTS does not provide anonymous or unverified voice services. Every customer able to originate voice traffic on the RWTS platform passes identity and legitimacy verification before service is activated.

At onboarding, RWTS:

1. Verifies the customer's legal identity. RWTS currently provides voice services only to Australian-registered entities; a number of these are the Australian operations of global organisations, but the contracting customer is in every case an Australian-registered entity. Verification includes validation of the Australian Business Number (ABN) or Australian Company Number (ACN) against the Australian Business Register, confirmation of the entity's registration status, and identification of the contracting officer. If RWTS in future accepts an overseas-registered customer, equivalent company-registry verification will apply.
2. Verifies the identity of the individual establishing the account, consistent with RWTS's obligations under the C661 code and ACMA customer identity verification requirements.
3. Establishes the customer's intended use of the service, including expected call volumes, destinations and calling patterns. Customers whose intended use involves outbound campaigns, contact-centre operation or automated dialling are subject to enhanced due diligence, including review of the customer's consent and compliance practices, before any such use is approved in writing.
4. Conducts a credit assessment, which provides an additional identity and legitimacy control.

On an ongoing basis, RWTS: re-validates customer details when service changes are requested, monitors for material changes in traffic behaviour inconsistent with the customer's stated use (see Traffic Monitoring below), and refreshes due diligence for customers flagged by monitoring or by external intelligence.

Contractual controls. RWTS's standard terms and Acceptable Use Policy prohibit the use of its services to originate illegal robocalls, to transmit inaccurate or misleading calling line identification, or to contravene applicable telemarketing and anti-spam law — including, for traffic terminating in the United States, the Telephone Consumer Protection Act and the Truth in Caller ID Act. The terms entitle RWTS to suspend or terminate service immediately and without compensation where it reasonably suspects breach.

Calling Line Identification Controls

RWTS operates its own voice platform and controls calling line identification (CLI) presentation at the platform level.

- Customers may only present CLIs that RWTS has allocated to them, or numbers the customer has demonstrated it is authorised to use. Authorisation for customer-supplied numbers requires evidence of the customer's right to use the number before it is provisioned.
- CLI presentation is enforced by allow-list on the RWTS voice platform. Calls attempting to present a CLI outside the customer's authorised set are **rejected** — they do not leave the RWTS network with the unauthorised CLI. This mirrors RWTS's domestic obligations: the C661 code requires Australian providers to block calls carrying invalid or unauthorised calling line identification.
- RWTS does not offer arbitrary CLI spoofing or "CLI flexibility" products.

These controls mean that traffic leaving the RWTS network carries CLI that is traceable to an identified, verified customer.

Traffic Monitoring and Analytics

RWTS operates its voice platform and network directly and performs all traffic analysis in-house on its own infrastructure. No third-party analytics or fraud-management service is engaged. The monitoring stack combines VoIPmonitor (packet-level and call-quality analysis across the voice platform) with detection systems RWTS has developed and operates itself, running over its own call detail records (CDRs). Monitoring includes:

- **Volumetric analysis** — per-customer call volumes measured against the customer's established baseline and stated use, with alerting on abnormal spikes, including out-of-hours origination inconsistent with the customer's business profile.
- **Call-pattern indicators of robocalling and fraud** — including abnormal ratios of short-duration calls, low answer-seizure ratios, high volumes to sequential or distributed number ranges, and unusual destination concentration.
- **Fraud and toll-abuse controls** — custom-built toll fraud detection with per-customer rate and concurrency limits, destination controls, and automated alerts feeding RWTS's network operations team for review and action.
- **Spend-pattern analysis** — per-customer spend tracked against historical baselines, surfacing compromise and abnormal campaign behaviour that volumetric measures alone can miss.
- **Scatter analysis** — analysis of the distribution of called numbers per customer, identifying the wide, shallow calling patterns characteristic of robocall campaigns as distinct from ordinary business calling.
- **Robocall-specific detection** — purpose-built detection developed by RWTS combining the above signals to flag suspected robocall origination for immediate operational review.

Alerts are reviewed by RWTS engineering and operations staff. Because RWTS operates the platform itself, it can act on findings immediately — including suspending a customer's origination capability — without dependence on an upstream vendor.

Traceback Cooperation

RWTS commits to **respond fully, and within 24 hours, to all traceback requests** from the Federal Communications Commission, civil and criminal law enforcement, and the registered industry traceback consortium (the Industry Traceback Group operated by USTelecom), and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.

- Traceback requests are handled by the contact identified in this filing and below. Requests are actioned as priority operational incidents, not routine correspondence.
- Because CLI on the RWTS platform is allow-listed to verified customers, RWTS can identify the originating customer for any call it has carried from its CDRs.
- RWTS retains CDRs for a minimum of two years, consistent with its Australian data retention obligations, ensuring traceback requests can be answered for historical traffic.

- RWTS already performs the equivalent function domestically: the C661 code obliges Australian providers to trace scam calls to their source and share findings with other providers and ACMA.

Robocall mitigation and traceback point of contact:

Name	Andrew Yager
Title	Managing Director
Email	noc@rwts.com.au (monitored by RWTS network operations)
Telephone	+61 2 9037 0500

Mitigation and Enforcement Procedures

When RWTS is notified — by the Commission, the Industry Traceback Group, a downstream provider, ACMA, or its own monitoring — that traffic originating from its network is suspected of being illegal robocall traffic, RWTS will:

- 1. Acknowledge and investigate within 24 hours**, identifying the originating customer, the affected traffic, and the CLI(s) involved from platform records.
- 2. Suspend the originating capability** of the identified customer or service where the evidence indicates illegal robocalling, pending investigation. Suspension is applied at the platform level and is effective immediately.
- 3. Block identified traffic** where a specific pattern, CLI or destination set can be isolated without suspending unrelated legitimate services.
- 4. Terminate service** for confirmed, deliberate or repeat originators of illegal robocall traffic, and decline future service to the responsible parties.
- 5. Report back** to the notifying party on the action taken, and notify ACMA or other Australian authorities where Australian law requires or permits.

These procedures apply equally to retail customers and to wholesale customers sending traffic through RWTS. Wholesale trunk groups can be suspended or blocked from US destinations at the platform level without affecting other customers' services, and the additional controls described in the Wholesale Customers section below apply.

Wholesale Customers — Know-Your-Upstream-Provider Controls

RWTS provides wholesale voice connectivity to other providers who send calls through the RWTS network. Where that traffic is destined for the United States, RWTS neither originates nor terminates it

and acts as a non-gateway intermediate provider. RWTS applies the following controls to that traffic, consistent with 47 CFR § 64.6305(f):

- 1. Identity and verification.** Wholesale customers are identified and verified to the same standard as retail customers. The full know-your-customer process described above applies, including verification of the entity, its officers, and its intended traffic profile.
- 2. RMD filing requirement.** Before RWTS enables routing to United States destinations for a wholesale customer, that customer must hold its own current certification in the Robocall Mitigation Database. RWTS verifies the customer's RMD filing status before enabling US-destined routing and periodically thereafter. US-destined routing is withdrawn for any wholesale customer whose RMD filing is removed by Commission action or otherwise lapses.
- 3. Contractual parity of care.** Wholesale customers sending US-destined traffic must contractually commit to operate a robocall mitigation program applying at least the same level of care as the program described in this document, including customer verification, calling line identification controls, and a commitment to respond fully and within 24 hours to traceback requests.
- 4. Monitoring and enforcement.** The traffic monitoring described above is applied per wholesale customer. RWTS can suspend a wholesale customer's US-destined routing, or the customer's service entirely, at the platform level and with immediate effect.
- 5. Traceback.** For traffic RWTS carries as an intermediate provider, RWTS identifies the immediate upstream provider from its call detail records and provides that identification in traceback responses within 24 hours, enabling continued traceback to the originating provider.

Program Review

This program is reviewed at least annually, ahead of the RMD annual recertification window (which opens on 1 February each year, with recertification due by 1 March), and additionally whenever there is a material change to RWTS's services, platform, customer base or the applicable US or Australian regulatory framework. The version of this document on file with the RMD is the current statement of RWTS's robocall mitigation program.

Declaration of Accuracy

The contents of this Robocall Mitigation Program Description are true and correct to the best of the knowledge of the officer executing the accompanying RMD certification. Nothing in this document is designated confidential; RWTS has not requested confidential treatment of any portion of this filing.

Real World Technology Solutions Pty Ltd — ABN 74 101 234 664 — Macquarie Park, NSW, Australia