

Robocall Mitigation Program Description

IT Noble Inc.

Prepared: February 13, 2026

Provider Name	IT Noble Inc.
Business Address	800 E. Rochambeau Drive Suite F, 511, Williamsburg, VA 23188
Business Phone	757-903-2414
FCC Registration Number (FRN)	0028307247
Provider Type	Voice over Internet Protocol (VoIP) service provider / reseller (not a wholesaler)
Purpose of Document	Robocall Mitigation Database (RMD) filing requirement – program description

1. Overview

IT Noble Inc. provides interconnected and/or non-interconnected VoIP services as a reseller. IT Noble Inc. is committed to preventing the origination, routing, and transmission of illegal robocalls on its network and to ensuring that any traffic it introduces into the public switched telephone network (PSTN) is lawful. This document describes the Robocall Mitigation Program (RMP) implemented by IT Noble Inc. to comply with the Federal Communications Commission (FCC) requirements for providers filing in the Robocall Mitigation Database (RMD).

2. Governance and Responsible Personnel

IT Noble Inc. maintains internal accountability for robocall mitigation. The company's designated compliance point of contact is responsible for maintaining this program, reviewing carrier notifications, responding to traceback requests, and coordinating with upstream providers and customers as needed. IT Noble Inc. also maintains internal procedures for documenting complaints, escalations, and corrective actions.

3. Traffic Source and Business Model

IT Noble Inc. operates as a VoIP service provider reseller. IT Noble Inc. does not operate as a wholesale originating carrier and does not provide open public origination for unknown parties. Traffic is introduced to the PSTN through upstream voice service partners. IT Noble Inc. may provide service to business and/or residential end users and business customers using VoIP service. Customers may use assigned telephone numbers or may port numbers into the service.

4. Robocall Mitigation Measures

IT Noble Inc. uses a layered approach to mitigate illegal robocalls. The controls below are applied to the extent technically feasible for a reseller, and in coordination with upstream providers:

- **Customer vetting and onboarding controls.** IT Noble Inc. verifies customer identity and collects sufficient information to support lawful service use. Higher-risk customer types and use cases receive enhanced scrutiny.

- **Acceptable Use Policy (AUP) and contractual restrictions.** Customer agreements prohibit illegal robocalls, caller ID spoofing, and any use that violates the Telephone Consumer Protection Act (TCPA), the Truth in Caller ID Act, or FCC rules.
- **Network monitoring and traffic analytics.** IT Noble Inc. monitors call patterns and call volumes for anomalies consistent with illegal robocall campaigns, including high call attempts, short-duration calls, high answer-seizure ratios, and repeated calling to sequential or random numbers.
- **Complaint intake and escalation.** IT Noble Inc. logs and reviews consumer complaints, carrier notifications, and third-party reports. Complaints are investigated and correlated with call records.
- **Blocking and suspension procedures.** When illegal robocall activity is suspected or confirmed, IT Noble Inc. may block calls, suspend service, terminate accounts, or require remediation before restoring service.
- **STIR/SHAKEN coordination.** As a reseller, IT Noble Inc. works with upstream providers to ensure that outbound calls are signed and/or that appropriate attestation levels are applied where supported. IT Noble Inc. supports the use of STIR/SHAKEN authentication information and respects verification results and downstream analytics.
- **Traceback cooperation.** IT Noble Inc. cooperates with the Industry Traceback Group and with upstream and downstream providers. IT Noble Inc. responds to traceback requests in a timely manner and provides call detail records (CDRs) or other information consistent with legal and contractual obligations.
- **Do-Not-Originate (DNO) and high-risk number protections.** IT Noble Inc. supports the use of DNO lists and heightened scrutiny for numbers associated with government agencies, financial institutions, and other frequently spoofed entities where feasible through upstream partners.
- **Recordkeeping.** IT Noble Inc. retains relevant records, including customer onboarding documentation, call detail records, complaint logs, and mitigation actions for a commercially reasonable period, consistent with legal requirements and vendor capabilities.

5. STIR/SHAKEN Implementation Status

IT Noble Inc. is a reseller VoIP provider and therefore may not directly operate the signing infrastructure for STIR/SHAKEN. IT Noble Inc. coordinates with its upstream service provider(s) to support STIR/SHAKEN for outbound traffic. Where IT Noble Inc. is the direct provider for end-user customers, it requires that outbound calls be transmitted via upstream partners that support STIR/SHAKEN, and it works to ensure that the appropriate attestation level is applied based on customer relationship and number assignment/verification. If full STIR/SHAKEN signing is not technically feasible for certain traffic, IT Noble Inc. relies on the mitigation measures described in this document to reduce the risk of illegal robocalls.

6. Response to Notifications, Complaints, and Tracebacks

IT Noble Inc. maintains procedures to respond to:

- **Carrier notifications** regarding suspected illegal traffic
- **Industry Traceback Group (ITG) requests**
- **Consumer complaints** received directly or through third parties
- **Law enforcement or regulatory inquiries**

Upon receipt, IT Noble Inc. reviews the complaint or traceback request, identifies the associated customer or traffic source, and takes appropriate action. Actions may include requesting customer explanation,

implementing call blocking, reducing call rates, suspending or terminating service, and/or escalating to upstream partners. IT Noble Inc. documents investigative steps and outcomes.

7. Ongoing Program Maintenance

IT Noble Inc. reviews its robocall mitigation controls periodically and updates procedures as necessary to reflect changes in FCC rules, industry best practices, vendor capabilities, and evolving robocall tactics. IT Noble Inc. trains relevant personnel on complaint handling, traceback response, and escalation procedures.

8. Certification Statement

IT Noble Inc. certifies that it has implemented the robocall mitigation program described herein and that it will take reasonable steps to prevent the origination of illegal robocalls on its network. IT Noble Inc. further certifies that it will cooperate in traceback efforts and respond to requests from the FCC, law enforcement, and industry traceback entities, consistent with applicable law.

Authorized Representative (typed name): Mark T Moore

Title: President

Signature: [Handwritten Signature]

Date: 2/13/20

Note: This document is provided as a compliance program description for RMD filing purposes. IT Noble Inc. should ensure that the information reflects its actual practices and vendor relationships.