

Robocall Mitigation Certification and Mitigation Plan

1. Company Information

Company Name: Inet Technologies Inc.

Business Address: 539 W Commerce St, Ste 192, Dallas, TX 75208

Contact Information:

Name: Tim Wilson

Title: CEO/Engineer

Email: twil@icallsystems.com

Phone: (817) 769-2202

2. Certification

We certify the following:

1. All calls originating on our network are subject to a robust robocall mitigation program.
2. No prior certification has been removed by Commission action, and we are not prohibited from filing in the Robocall Mitigation Database (RMD).
3. STIR/SHAKEN Implementation Status:
 - Current Status: Partially implemented through carrier partner.
 - All calls originating from our network are currently signed by our carrier partner to meet caller identification verification standards.

3. Robocall Mitigation Plan

3.1 Customer Screening and Monitoring

1. Dialers and dialer traffic are prohibited as per our customer agreements.
2. Measures are in place to screen and monitor new and renewing customers to prevent illegal robocalls.
3. Caller ID settings are actively managed to ensure all Caller IDs have a matching telephone number on file, configured and maintained by Inet Technologies Inc.

3.2 Call Analytics Systems

1. Hosted PBX statistics are used to calculate calls per minute with a threshold of 5 calls/min per user.

2. Carrier-side fraud detection measures include monitoring for Short Duration Notifications (calls under six seconds).

3. Utilize advanced analytical platform such Metabase identify excessive usage, call patterns, misconfiguration.

3.3 Upstream Provider Compliance

No services are sold to upstream providers; we exclusively serve local small businesses.

3.4 Traceback Response Commitment

Dedicated personnel address traceback requests within 24 hours.

3.5 Role in the Call Chain

As a Voice Service Provider, we originate calls and ensure robust mitigation measures to prevent illegal traffic.

4. Implementation Details

4.1 Current Status

Operating Company Number (OCN) obtained as part of the STIR/SHAKEN implementation process.

4.2 Next Steps

1. Acquire a Service Provider Code (SPC) token to access the STIR/SHAKEN ecosystem.
2. Apply for a digital certificate from a Secure Telephone Identity Certification Authority (STI-CA).

4.3 Timeline

Complete SPC token acquisition and certificate request within 60 days.

Fully integrate call signing capabilities by 1/30/2025.

5. Mitigation Practices

1. Thorough customer vetting.
2. Carrier partner's signing services ensure compliance during the transition phase.
3. Call analytics and IP blocking implemented for specific regions.
4. Analytical systems include:
 - Metabase
 - FusionPBX Call Statistics
 - Short Duration Notifications

6. Mitigation Strategies for Non-STIR/SHAKEN Calls

1. Use call analytics to detect suspicious patterns.
2. Deploy automated tools such as fail2ban to block or flag registrations / calls resembling illegal robocalls.

7. Compliance and Review Process

1. Monthly audits of call logs and reports to ensure thresholds are maintained.
2. Quarterly review and documentation updates by the compliance team.

8. Prior Investigations or Actions

No investigations or enforcement actions within the past two years.

9. Commitment

We are committed to achieving full compliance with the STIR/SHAKEN framework and maintaining a secure calling environment for our customers.

10. Authorized Signature

Tim Wilson

CEO/Engineer

Inet Technologies Inc.

Date: December 11, 2024

11. FCC Filing Confirmation

We confirm that this Robocall Mitigation Plan has been or will be filed in the FCC's Robocall Mitigation Database (RMD) in accordance with regulatory requirements. Any updates to this plan will be promptly submitted to the FCC to maintain compliance.

12. Consumer Protections

To further protect our customers, we are committed to providing education and tools to help them recognize and avoid illegal robocalls. These initiatives include:

1. Educational resources to inform customers about common robocall scams.
2. Tools and services such as spam filters and call-blocking features to enhance customer protection.
3. Dedicated support channels to address customer concerns related to suspicious or fraudulent calls.