



Robocall Mitigation Program Description

Dex Imaging LLC (“Dex” or “Company”) has implemented a Robocall Mitigation Program designed to prevent the origination, transmission, and termination of illegal robocalls, including spoofed and fraudulent traffic, in accordance with FCC rules and the TRACED Act.

1. Commitment to Robocall Mitigation

Dex is committed to actively mitigating illegal robocalls and ensuring compliance with all applicable FCC regulations. The Company takes reasonable and effective steps to identify, monitor, and address unlawful or suspicious voice traffic on its network.

2. Customer Due Diligence and Vetting

The Company employs reasonable **Know-Your-Customer (KYC)** practices prior to onboarding customers, which may include:

- Collection and verification of customer identity information
- Review of the customer’s intended use of voice services
- Contractual prohibitions against illegal robocalling, spoofing, and fraud

Customers found engaged in illegal or abusive calling practices are subject to suspension or termination of service.

3. Traffic Monitoring and Analytics

The Company monitors voice traffic patterns on its network to identify indicators of potential illegal robocalls, including but not limited to:

- Abnormally high call volumes
- Short call duration patterns
- Invalid, unassigned, or spoofed calling numbers

- Consumer complaints or carrier notifications

When suspicious activity is identified, the Company investigates and takes appropriate remedial action.

4. Response to Traceback and Enforcement Requests

Dex cooperates fully and promptly with:

- The FCC
- The Industry Traceback Group (ITG)
- Law enforcement agencies
- Downstream and upstream carriers

The Company responds to traceback requests within required timeframes and takes corrective action when illegal traffic is confirmed.

5. Blocking and Mitigation Actions

Upon identifying confirmed or suspected illegal robocall traffic, the Company may:

- Block calls or calling numbers
 - Require remediation from the customer or upstream provider
 - Suspend or terminate service
 - Refuse to accept traffic from non-compliant providers
-

6. STIR/SHAKEN Implementation Status

Where technically feasible, the Company has implemented STIR/SHAKEN authentication for voice traffic on its IP networks.

For traffic or network segments where STIR/SHAKEN is not currently feasible, this Robocall Mitigation Program is used to reduce the risk of illegal robocalls until full implementation is achieved.

7. Program Review and Updates

This Robocall Mitigation Program is reviewed periodically and updated as necessary to reflect:

- Changes in FCC rules or guidance
 - Industry best practices
 - Technological advancements in call authentication and analytics
-

8. Certification

Dex certifies that it has implemented this Robocall Mitigation Program in good faith and that the program is reasonably designed to prevent illegal robocalls from originating on or transiting its network.