

1. **Caller ID Authentication:** Implement STIR/SHAKEN or other call authentication technologies to validate caller ID information and reduce spoofing.
2. **Network Monitoring:** Regularly monitor network traffic to identify patterns or anomalies indicating illegal robocalls.
3. **Customer Vetting:** Establish strict Know Your Customer (KYC) processes to prevent fraudulent customers from using the network for illegal robocalling.
4. **Traceback and Enforcement:** Respond to traceback requests from law enforcement and take appropriate actions against customers engaging in illegal robocalling.
5. **Consumer Protection:** Offer call-blocking and labeling services to help consumers identify and avoid unwanted calls.
6. **Partnerships:** Collaborate with other voice service providers, industry organizations share best practices and strengthen collective efforts against illegal robocalls.
7. **Education and Training:** Provide ongoing training to employees on identifying and preventing illegal robocalls, and educate customers about the risks and prevention measures.
8. **Adaptive Measures:** Continuously adapt and update the RMP to address evolving threats and emerging technologies, ensuring ongoing effectiveness in mitigating illegal robocalls.