Updated Robocall Mitigation Strategy (RMD) – Renvyo

A robust Robocall Mitigation Strategy is essential to comply with current FCC rules, maintain access to U.S. telecommunications networks, and protect customers from illegal robocalls. This plan reflects updated regulatory expectations and enforcement priorities through 2025.

---

1. Stay Aligned with Evolving FCC Regulations

- Continuously monitor FCC orders, public notices, and rule changes related to robocall mitigation and STIR/SHAKEN implementation.
- Assign a compliance lead to track new deadlines, enforcement actions, and guidance updates.
- Regularly update internal policies to reflect the latest FCC rulemakings and industry standards.

---

2. Strengthen Caller ID Authentication (STIR/SHAKEN)

- **Ensure full compliance with the FCC's STIR/SHAKEN requirements** by obtaining your own Service Provider Code (SPC) token and digital certificates from a STIR/SHAKEN Certificate Authority.
- *Do not* rely on third-party SPC tokens or certificates without proper FCC-required documentation — each provider must make key attestation decisions and sign calls with its own certificate (not a third party's) to be compliant.

---

3. Enhance Your Robocall Mitigation Plan

- Submit a detailed **Robocall Mitigation Plan** to the FCC's Robocall Mitigation Database (RMD) that includes:
    - Step-by-step procedures to prevent illegal robocalls.
    - How STIR/SHAKEN is implemented and verified.
    - Effective traceback and call-pattern monitoring processes.
- Update your RMD submission whenever there are material changes to your systems or mitigation approaches.

4. Maintain Accurate and Timely RMD Filings

- File or **update your RMD certification** with all required information by the FCC's deadlines (note that failure to update can lead to removal from the RMD and network disconnection).
- Implement internal checks to ensure:
    - Contact details and corporate information in the RMD match CORES filings.
    - Annual re-certification deadlines are met.
    - Any changes are updated within required timeframes to avoid penalties.

---

5. Deploy Advanced Call Blocking and Filtering

- Use up-to-date call blocking and traffic filtering tools to reduce illegal calls reaching your customers.
- Maintain and regularly refresh lists of known scam call numbers and patterns.
- Employ analytics to detect high-volume patterns typical of illegal robocall campaigns.

---

6. Monitor and Respond to Call Traffic Anomalies

- Apply automated tools to identify suspicious calling behavior (e.g., sudden spikes in volume or unusual destinations).
- Integrate real-time alerts so that suspected illegal traffic prompts investigation and corrective action.

---

7. Secure Explicit Consent and Maintain Records

- Before placing calls to individuals, ensure explicit consent (e.g., documented opt-in) and retain detailed records (date, time, method of consent).
- Track all customer interactions to defend against TCPA complaints and related enforcement actions.

---

8. Offer Robocall Mitigation Services to Customers

- Provide customers with optional robocall protection services, clearly explaining benefits such as reduced nuisance calls and improved call legitimacy.
- Promote transparency in how your systems reduce unwanted calls.

9. Encourage Reporting and Collaborate on Enforcement

- Train employees and educate customers on how to report suspected illegal calls to the FCC.
- Cooperate with law enforcement, industry tracebacks, and regulatory investigations when needed.

---

10. Maintain Detailed Internal Compliance Records

- Archive internal call logs, timestamps, STIR/SHAKEN attestation data, and RMD submission histories.
- Implement documentation procedures that demonstrate proactive compliance with both FCC robocall and TCPA rules.

---

11. Conduct Regular Strategy Reviews

- Perform quarterly reviews of your robocall mitigation strategy.
- Adjust processes based on enforcement trends — including recent FCC removals of non-compliant providers from the RMD — to avoid disruptions.

---

12. Communicate Your Compliance to Stakeholders

- Publicly share your dedication to FCC compliance on your website and in customer communications.
- Offer transparency about caller authentication, mitigation efforts, and protective services.

---

13. Consult Telecom Regulatory Experts

- Work with specialized telecommunications attorneys or compliance consultants to interpret FCC rules and tailor your mitigation plan.
- Regular legal oversight can prevent costly RMD deficiencies, penalties, or network access loss.

By implementing this updated Robocall Mitigation Strategy aligned with the **latest FCC requirements and enforcement actions**,**Renvyo** will improve regulatory compliance, reduce illegal robocall exposure, and build credibility with customers and telecom partners.
