

YakPath Robocall Mitigation Plan

YakPath is dedicated to preventing illegal robocalls from originating, transiting, or terminating on our network. Our mitigation program complies with FCC regulations under **47 CFR § 64.6305** and reflects our commitment to transparency, compliance, and customer trust.

1. Certification of Compliance

YakPath certifies the following:

- All calls originating on our network are subject to our robocall mitigation program.
- No prior certification has been removed by FCC action, and we are not prohibited from filing in the Robocall Mitigation Database (RMD).
- YakPath is committed to fully responding to traceback requests from the ITG, the TPTG, the FCC, and law enforcement within 24 hours. YakPath will co
- **STIR/SHAKEN Implementation:**
 - We have fully implemented STIR/SHAKEN.
 - All traffic on our network is IP-based.
- YakPath is fully committed to cooperating with the Federal Communications Commission (FCC), law enforcement, and the industry traceback consortium, including the Industry Traceback Group (ITG) and other relevant entities, to investigate and stop illegal robocallers using our services to originate or transit calls into the United States and its territories.

2. Traceback Cooperation and Reporting

- YakPath commits to fully responding within **24 hours** to all traceback requests from the ITG, the FCC, law enforcement, and other relevant organizations.
- YakPath cooperates in investigations to identify and stop illegal robocallers from using our services to originate or transit illegal calls.
- Upon receiving written notice from the FCC's Enforcement Bureau identifying illegal traffic, YakPath will:
- Block and report the identified illegal traffic and any substantially similar traffic on an ongoing basis unless an investigation determines the traffic is not illegal.

- Provide the Enforcement Bureau with an explanation if YakPath concludes the identified traffic is not illegal, including the steps taken to reach that determination.

3. Traffic Monitoring and Analytics

- YakPath uses a combination of internal tools, third-party solutions, and data analytics to detect and address illegal robocalls. These efforts include:
- Checking for **Do Not Originate (DNO)** numbers to ensure they are not used for outbound calls.
- Detecting invalid phone number formats, unassigned number blocks, and unauthorized area codes.
- Monitoring network traffic to identify irregular or unexpected calling patterns that deviate from customer profiles.

4. Know Your Customer (KYC) Policy

- To prevent misuse of our network, YakPath enforces a rigorous **Know Your Customer (KYC)** process, which includes:
 - **Personal Vetting:**
 - YakPath personnel have direct, on-site interaction with every customer, gaining firsthand knowledge of their business operations and telecommunication needs.
 - **Restricted Customer Base:**
 - YakPath does not offer services to unknown entities or engage in unsolicited business. Each customer relationship is built on long-standing trust and familiarity.
 - **Prohibited Activities:**
 - YakPath contracts explicitly prohibit automated calling and other high-risk activities, further safeguarding our network from misuse.
 - Monitoring network activity to identify suspicious traffic patterns.
 - Limiting customer capacity through call-per-second and concurrent session limits.

- Regularly reviewing customer call patterns for potential abusive traffic.
- Verifying new customers through a combination of:
- Electronic and manual verification systems.
- Credit reviews and references from trusted industry members.
- Previous experiences with customer executives and employees.
- Restricting the capabilities of new accounts until all verification processes are complete.

5. Upstream Provider and Customer Traffic Management

- YakPath works with Flowroute as the upstream provider for voice traffic and reserves the right to:
 - Refuse traffic from any party if robocalling or the use of invalid or unauthorized originating numbers is identified or suspected.
 - Block originating numbers, terminating numbers, trunks, or customers involved in illegal activity, including terminating relationships with customers who engage in such practices.

6. STIR/SHAKEN Implementation Details

- **Inbound Calls:**
 - Our upstream provider, Flowroute, provides STIR/SHAKEN-based insights for inbound calls, including:
 - **TN Validation Results:**
 - TN-Validation-Passed, TN-Validation-Failed, or No-TN-Validation, presented via the verstat parameter in SIP headers (PAI or FROM).
 - When TN-Validation-Passed is received:
 - “[V]” is prepended to the CNAM to denote validation.
 - If no CNAM is provided or it is blank, “[V]” is used as the CNAM.

- Flowroute ensures CNAM integrity by overwriting invalid content.
- **Policy Note:** Inbound calls are not blocked based on validation results.
- **Outbound Calls:**
 - Flowroute assigns attestation levels for outbound calls as follows:
 - **Attestation A:** Calls from TNs purchased from Flowroute and associated with the specific customer account.
 - **Attestation B:** Calls from TNs not purchased from Flowroute.
 - **Attestation C:** Calls from customers in 'Pending' status, toll-free numbers not hosted on Flowroute, invalid TNs, or calls with "Anonymous" caller ID.
 - **Transparency:** Flowroute passes through, unaltered, any attestation received on calls arriving at their platform.
 - **Policy Note:** Outbound calls are not blocked based on attestation levels.

7. SIP Configuration and Header Parsing Policy

YakPath customers cannot modify SIP configurations, ensuring compliance with our policies and maintaining the integrity of our network. All SIP configurations, including caller ID settings and routing logic, are fully managed by YakPath to maintain security and compliance with regulatory requirements.

However, Flowroute allows its customers to parse SIP headers for read-only purposes. This means that YakPath, as a customer of Flowroute, can analyze information contained in SIP headers, such as the verstat parameter or CNAM data, to apply custom treatment within their systems. For example:

- **Parsing Validation Results:** Flowroute customers can interpret verstat values (TN-Validation-Passed, TN-Validation-Failed, or No-TN-Validation) to decide how to handle or log calls.
- **Displaying Caller Information:** Flowroute customers can use CNAM data provided by Flowroute for display purposes.

YakPath customers do not have the ability to parse or modify SIP headers, ensuring that all interactions with SIP data are securely managed within YakPath's systems and policies.

8. Network Traffic Analysis

- **SIP Configuration Management:**
 - All clients use SIP phones or mobile applications configured exclusively by YakPath.
 - Customers cannot modify SIP configurations, ensuring compliance with our policies.
- **No Trunking Services:**
 - YakPath does not provide trunking services, limiting the risk of misuse.
- **IP Connection Control:**
 - Each SIP extension is authorized for a single IP connection at a time.
- **Upstream Carrier Alerts:**
 - Flowroute monitors traffic patterns and alerts YakPath for calls exceeding predefined thresholds, enabling prompt investigation and action.

9. Real-Time Blocking

- **Automatic Blacklisting:**
 - Any IP attempting more than five failed authentications to our SIP gateway is blocked for 24 hours.
- **Caller ID Integrity:**
 - SIP extensions cannot override YakPath-assigned DID or caller ID settings, preventing manipulation of call source data.

10. Customer Notification Policy

YakPath ensures that customers are aware of their responsibilities through:

- **Initial Onboarding Notification:**
 - Customers receive a comprehensive email outlining caller ID policies and compliance requirements.
- **Periodic Reminders:**
 - Annual emails provide regulatory updates and reinforce compliance.

- Targeted outreach is conducted for customers with potentially non-compliant usage patterns.
- **Proactive Alerts:**
 - Customers are notified promptly if violations are detected, with details of corrective actions required.
- **Educational Resources:**
 - YakPath provides access to compliance materials and customer support.
- **Notification Tracking:**
 - All notifications are logged for transparency and accountability.

11. Traceback Cooperation

YakPath is committed to full cooperation with the FCC, law enforcement, and the industry traceback consortium to investigate and mitigate illegal robocall activity.

- YakPath pledges to respond to traceback requests within 24 hours of receipt.
- A dedicated compliance officer is responsible for managing traceback inquiries and ensuring timely, accurate responses.
- Our process includes reviewing call records, identifying relevant traffic patterns, and taking corrective actions as needed.

12. Call Analytics Systems

YakPath utilizes a combination of tools and practices to monitor and analyze call traffic for anomalies or patterns indicative of illegal robocalls:

- **Flowroute Tools:** YakPath leverages Flowroute's Call Detail Records (CDRs) to identify and analyze call behaviors such as high call volumes, short durations, or repeated invalid numbers.
- **Firewall Security:** Advanced firewall settings are used to detect and block suspicious traffic, including unauthorized access attempts and anomalous usage patterns.
- **Anomaly Detection:** YakPath actively monitors network activity for irregular traffic patterns and investigates any deviations promptly, ensuring compliance with regulatory standards.

Appendix A – Email Template to Inform Customers About the Importance of Valid Caller ID Information

Subject: Important Notice: Responsible Use of Caller ID Information

Dear [Customer_Name],

We are reaching out to remind you of the importance of using valid caller ID information and adhering to industry regulations to prevent the misuse of telecommunications services.

As part of our commitment to maintaining a secure and reliable network for all users, we want to emphasize the following:

1. Valid Caller ID Information

Using accurate and valid caller ID information is critical. It ensures transparency in your communications and helps build trust with the recipients of your calls.

- **What this means for you:**
 - Ensure the numbers displayed in the caller ID field are assigned to you or authorized for your use.
 - Avoid using unassigned, spoofed, or misleading numbers in your outbound calls.

2. Compliance with Robocall Regulations

The Federal Communications Commission (FCC) has strict rules against the origination of illegal robocalls. Calls that violate these rules may be subject to penalties and enforcement actions.

- **Consequences of non-compliance:**
 - Calls with invalid or spoofed caller ID information may be blocked by other providers.
 - You could face fines or other legal repercussions if found originating illegal robocalls.

3. Our Commitment to Mitigation

We are actively monitoring call traffic to detect and prevent the transmission of unlawful robocalls. This includes cooperating with the FCC and industry traceback initiatives.

4. Your Role in Responsible Use

We request your cooperation in:

- Ensuring that all calls originating from your system comply with FCC rules.
- Reviewing your call practices to prevent the transmission of any unlawful robocalls.
- Informing us immediately if you suspect any misuse of your account or system.

Questions or Concerns?

If you have any questions about these requirements or need assistance in ensuring compliance, please don't hesitate to contact us at accountspayable@yakpath.com or (407) 531-8552.

Thank you for your attention to this important matter. Together, we can maintain a trusted and secure telecommunications environment.

Best regards,

[Your_Email_Signature]