[Revised Robocall Mitigation Plan – KYC Section]

1. Customer Identification and Verification (KYC)

Bright Packet, Inc. implements a comprehensive Know Your Customer (KYC) program prior to onboarding any new customer and on an ongoing basis for existing customers.

a. Customer Information Collection

Before activating service, Bright Packet, Inc. collects and verifies the following information as part of its Know Your Customer (KYC) procedures:

• Legal business name and DBA (if applicable) are collected and verified to confirm the identity of the customer.

• Employer Identification Number (EIN) or Tax ID is collected and verified to confirm the legitimacy of the business entity.

• Physical business address is collected and verified (P.O. Boxes alone are not accepted) to confirm the operational presence of the customer.

• Authorized contact person information (including name, title, phone number, and email address) is collected and verified to ensure a responsible point of contact.

• Government-issued identification (such as a driver's license, passport, or state-issued ID) is verified for individuals or company principals. Such identification is reviewed and retained internally and is not submitted as part of this filing.

• Corporate registration documents (such as Articles of Incorporation, business registration certificates, or equivalent formation documents) are collected and verified to confirm the legal existence and good standing of the business entity. These documents are maintained internally in accordance with compliance policies.

• FCC Registration Number (FRN), if applicable, is collected and verified to confirm regulatory registration status.

• The nature of the customer's business and intended use of telecommunications services is collected and reviewed to assess expected traffic patterns and risk level

b. Risk Assessment and Customer Classification

Each customer is evaluated and assigned a risk level (Low, Medium, or High) as part of the Company's KYC procedures.

Risk classification is determined based on multiple factors, including:

• The nature of the customer's business (e.g., call centers, VoIP resellers, marketing or outbound calling activities)
• Expected traffic profile and calling patterns
• Geographic origination and termination patterns
• Any known compliance issues or prior regulatory or enforcement history
• Projected call volume and usage behavior

Based on this assessment, customers are categorized into risk tiers, which determine the level of monitoring and due diligence applied.

Customers identified as high-risk are subject to enhanced due diligence measures, including additional verification, closer traffic monitoring, and periodic review of account activity.

c. Enhanced Due Diligence (EDD)

Customers identified as high-risk are subject to enhanced due diligence procedures prior to and during service.

Enhanced due diligence measures may include:

• Additional verification of business identity and ownership
• Review of the customer's website, online presence, and business activities
• Verification through third-party or publicly available business databases
• Collection of additional supporting documentation, where applicable
• Confirmation of the customer's robocall compliance policies and intended use of services

High-risk customers are also subject to increased monitoring and periodic re-evaluation to ensure ongoing compliance.

2. Ongoing Monitoring and Analytics

Bright Packet, Inc. implements continuous monitoring of customer traffic to identify suspicious or potentially unlawful robocall activity.

Monitoring includes analysis of Call Detail Records (CDRs) and traffic patterns, including:

• Sudden spikes in call volume
• Unusual call duration patterns (e.g., short-duration or high-volume calls)
• Low answer-to-seizure ratios (ASR) or abnormal call completion rates
• Repeated call attempts to the same destination
• Traffic patterns inconsistent with the customer's stated business purpose

The Company utilizes internal monitoring tools and may leverage third-party analytics solutions to support detection and analysis of suspicious traffic.

Alerts generated through monitoring systems are reviewed and investigated by the Company.

3. Mitigation and Enforcement Actions

When suspicious or illegal robocall activity is identified, Bright Packet, Inc. takes prompt and appropriate action, including:

• Investigation of the identified traffic and customer activity
• Temporary suspension or restriction of suspicious traffic, where necessary
• Notification to the customer and request for explanation or remediation
• Blocking of specific traffic or termination of service for confirmed violations
• Cooperation with traceback requests and law enforcement or regulatory authorities

The Company applies these mitigation measures in a timely manner to prevent further transmission of unlawful robocalls.

4. Application to Existing Customers

Bright Packet, Inc. applies its KYC, risk assessment, and monitoring procedures not only to new customers but also to existing customers on an ongoing basis.

This includes:

• Periodic re-verification of customer information to ensure accuracy and validity
• Re-assessment of customer risk classification based on observed behavior and traffic patterns
• Ongoing monitoring and analysis of traffic patterns for anomalies or inconsistencies
• Immediate review and investigation upon detection of abnormal or suspicious traffic activity

These measures ensure that existing customers remain compliant with the Company's policies and applicable regulatory requirements.

5. Recordkeeping

Bright Packet, Inc. maintains records sufficient to demonstrate compliance with its robocall mitigation program and KYC procedures.

Such records include:

• Customer onboarding and verification documentation
• KYC verification results and risk assessments
• Monitoring data, including call detail records (CDRs), alerts, and traffic analysis
• Investigation records, including actions taken in response to suspicious or unlawful traffic

Records are retained and maintained internally in accordance with applicable FCC requirements and the Company's compliance policies.

6. Compliance Commitment

Bright Packet, Inc. is committed to full compliance with all applicable FCC rules and regulations, including 47 CFR § 64.6305.

The Company continuously reviews and updates its robocall mitigation program, KYC procedures, and monitoring practices to align with evolving regulatory requirements and industry best practices.