

Call Traffic Monitoring and Robocall Prevention Policy

Purpose

This policy outlines the procedures and practices used by ComData Solutions, Inc. for monitoring, reviewing, and analyzing call traffic to identify and block unlawful robocalls, as well as investigating patterns consistent with such activities.

Scope

This policy applies to all call traffic handled by ComData Solutions, Inc., including but not limited to calls originating from our network or passing through our systems.

Policy Overview

ComData Solutions, Inc. is committed to protecting its network and its customers from the harmful effects of unlawful robocalls. The company has implemented monitoring, reviewing, and analysis protocols to detect and block these calls effectively.

Monitoring Procedures

1. Call Traffic Monitoring

ComData Solutions, Inc. will continuously monitor call traffic across its network to detect patterns that may indicate unlawful robocalling activity. This will be done through automated systems that analyze call volumes, durations, and destinations.

2. Flagging Suspicious Activity

Specific criteria will be used to flag potential unlawful robocall activity, including, but not limited to:

- Unusual call volumes or frequencies
- Repeated short-duration calls
- High call volumes to known invalid or non-existent numbers
- Calls originating from suspicious or known unlawful robocall sources

3. Real-time Blocking

ComData Solutions, Inc. will use automated filtering technologies to block calls that meet specific criteria for unlawful robocalling. This includes the implementation of call authentication technologies such as SHAKEN/STIR to verify caller identities.

Reviewing Procedures

1. Regular Traffic Audits

Traffic audits will be conducted periodically to review patterns of call activity across the network. These audits will be designed to identify trends or anomalies indicative of robocalling practices.

2. Investigation of Reported Calls

Customer complaints and reports of unlawful robocalls will be investigated by reviewing

the relevant call records. This includes verifying the source of the call and determining whether it was appropriately flagged by the monitoring systems.

Analysis Procedures

1. **Trend Analysis**

ComData Solutions, Inc. will analyze aggregate call traffic data to identify larger trends that may indicate emerging robocall threats. This analysis will be used to refine and enhance our detection and blocking capabilities.

2. **Pattern Recognition**

The company will employ data analytics to identify specific calling patterns associated with unlawful robocalling campaigns. This may include analysis of geographic, time-based, and frequency-based patterns.

Blocking and Enforcement

1. **Immediate Blocking**

When unlawful robocalls are detected, ComData Solutions, Inc. will take immediate action to block the calls from reaching customers. The blocking actions will be automated where possible, but manual intervention may be required in some cases.

2. **Coordination with Authorities**

ComData Solutions, Inc. will coordinate with federal and state authorities, including the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC), to report unlawful robocall activities. Information regarding the source of the unlawful calls may be shared with these agencies to support broader enforcement actions.

Compliance and Reporting

1. **Regulatory Compliance**

ComData Solutions, Inc. will ensure that its call monitoring and blocking activities comply with all applicable laws and regulations, including the FCC's regulations on robocall prevention.

2. **Internal Reporting**

The company will maintain records of identified and blocked robocalls, including details on the volume and nature of the calls, as well as the actions taken to prevent them. These records will be reviewed on a regular basis to assess the effectiveness of the company's robocall prevention efforts.

Continuous Improvement

ComData Solutions, Inc. is committed to the continuous improvement of its robocall prevention measures. This will be achieved through regular review and updates to monitoring systems, data analysis techniques, and enforcement practices based on evolving threats and technological advancements.

Robocalling Mitigation Plan

Effective Date: [12/01/2024]

Last Reviewed: [12/01/2024]

Next Review Date: [12/01/2025]

Purpose

The purpose of this plan is to outline the procedures and practices implemented by ComData Solutions, Inc. to mitigate and combat illegal robocalling. This plan ensures compliance with federal regulations, including the Federal Communications Commission (FCC) requirements, and maintains the integrity of its communication network by preventing illegal robocalls.

Scope

This plan applies to all services provided by ComData Solutions, Inc., including voice services, and covers all customers, affiliates, and contractors engaged in transmitting voice communications through ComData Solutions, Inc.'s network. It addresses customer vetting, telephone number validation, and ongoing monitoring to identify and block illegal robocalls.

Policy Statement

ComData Solutions, Inc. is committed to preventing illegal robocalling activities on its network. This plan includes robust customer vetting procedures, telephone number validation processes, and continuous monitoring to detect, mitigate, and block illegal robocalls while ensuring that legitimate calls are not impacted.

1. Customer Vetting Procedures

1.1. Customer Registration and Onboarding

- All new customers are required to undergo a thorough vetting process before being granted access to ComData Solutions, Inc.'s services.
- The vetting process includes identity verification, validation of business registration information, and review of intended use cases for telephony services.
- Customers must sign a service agreement that includes a strict prohibition on the use of ComData Solutions, Inc.'s services for illegal robocalling and outlines the penalties for violations.

1.2. Enhanced Scrutiny for High-Risk Customers

- Customers who intend to use high volumes of outbound calls or who are in industries known for higher risks of robocalling (e.g., telemarketing) will undergo enhanced scrutiny.
- These customers must provide additional documentation, including a detailed description of call practices, opt-in procedures for call recipients, and compliance with federal regulations (e.g., Telephone Consumer Protection Act, TCPA).

1.3. Ongoing Customer Monitoring

- ComData Solutions, Inc. monitors customers' usage patterns and call volumes regularly to detect any suspicious activities indicative of illegal robocalling.
 - High-risk customers are subject to periodic audits to ensure compliance with the company's robocalling mitigation policies.
-

2. Telephone Number Validation

2.1. Number Assignment and Validation

- ComData Solutions, Inc. employs strict validation processes when assigning telephone numbers to customers.
- Before assigning numbers, the company ensures that the numbers are valid, have not been previously used for illegal robocalling, and are sourced from authorized pools of numbers.

2.2. STIR/SHAKEN Implementation

- ComData Solutions, Inc. has implemented the **STIR/SHAKEN** (Secure Telephone Identity Revisited/Signature-based Handling of Asserted Information Using toKENs) framework to validate the authenticity of caller ID information.
- All outbound calls are authenticated and verified through the STIR/SHAKEN protocol, preventing spoofed numbers from being used to originate illegal robocalls on the network.

2.3. Regular Number Audits

- ComData Solutions, Inc. conducts regular audits of the telephone numbers in use to ensure that they are being used for legitimate purposes and are compliant with the robocalling mitigation standards.
 - Numbers found to be associated with illegal activities are immediately revoked, and appropriate legal and regulatory action is taken.
-

3. Illegal Robocall Detection and Blocking

3.1. Call Analytics and Monitoring

- ComData Solutions, Inc. utilizes advanced call analytics tools to monitor call patterns and detect anomalous activities indicative of illegal robocalling.
- The company analyzes factors such as call duration, frequency, and recipient complaint patterns to identify potential illegal robocall campaigns.

3.2. Real-Time Blocking of Suspected Illegal Robocalls

- Once illegal robocalling activities are identified, ComData Solutions, Inc. employs real-time call blocking technologies to stop these calls from reaching recipients.
- Calls identified as originating from untrusted or spoofed sources are automatically blocked from traversing the network.

3.3. Collaboration with Industry Partners and Government Agencies

- ComData Solutions, Inc. collaborates with industry partners and government agencies, including the FCC, to share information about known robocallers and blocklists.
 - The company participates in robocalling mitigation initiatives and complies with all federal mandates regarding illegal robocall prevention.
-

4. Customer and Public Education

4.1. Customer Awareness Programs

- ComData Solutions, Inc. provides educational materials to customers regarding the risks of illegal robocalling and their obligations under the law.
- Customers are informed of best practices for staying compliant, including obtaining proper consent from call recipients and maintaining accurate records of such consents.

4.2. Public Reporting Mechanisms

- ComData Solutions, Inc. offers a mechanism for the public to report suspected illegal robocalls originating from its network.
 - Reports are investigated promptly, and appropriate measures are taken to prevent further illegal activities.
-

5. Enforcement and Penalties

5.1. Policy Violations

- Customers found to be engaging in illegal robocalling activities will face immediate suspension or termination of services.
- ComData Solutions, Inc. will cooperate with law enforcement and regulatory agencies in prosecuting those who engage in illegal robocalling.

5.2. Financial Penalties

- Customers involved in illegal robocalling may be subject to financial penalties in accordance with the service agreement and applicable laws.
-

6. Review and Auditing

6.1. Regular Audits

- ComData Solutions, Inc. will conduct regular audits of its robocalling mitigation efforts, customer vetting procedures, and telephone number validation processes to ensure ongoing effectiveness.

6.2. Plan Review

- This Robocalling Mitigation Plan will be reviewed and updated at least annually or as required by changes in regulations or industry best practices.
-

Approved by:

Johnny Kincanon
President

Date: 12/15/2024

Traceback Request Policy

Effective Date: [12/15/2024]

Last Reviewed: [12/15/2024]

Next Review Date: [12/15/2025]

Purpose

The purpose of this policy is to establish the procedures and guidelines that ComData Solutions, Inc. follows to respond to traceback requests related to suspected illegal robocalls. This policy ensures compliance with federal regulations, industry best practices, and collaboration with authorized traceback entities to identify and mitigate unlawful call traffic.

Policy Statement

ComData Solutions, Inc. is committed to combating illegal robocalling and will fully cooperate with traceback requests from authorized industry traceback consortiums, government agencies, and law enforcement entities. The company will provide timely, accurate, and complete responses to traceback requests in compliance with applicable laws and regulations.

Scope

This policy applies to all employees, contractors, and affiliates of ComData Solutions, Inc. who are involved in handling or processing traceback requests. It covers all voice traffic transmitted through the company's network, including calls originating, terminating, or transiting its systems.

Procedures for Handling Traceback Requests

1. Receipt of Traceback Request

- ComData Solutions, Inc. will only respond to traceback requests submitted by authorized entities, such as the Industry Traceback Group (ITG) or government agencies.
- All traceback requests must be sent to the designated contact point at ComData Solutions, Inc. via the official communication channel outlined below:
 - **Designated Email Address:** [Insert Email Address]
 - **Designated Phone Number:** [Insert Phone Number]

2. Verification of Request

- Upon receiving a traceback request, ComData Solutions, Inc. will verify the legitimacy of the request by confirming the identity and authority of the requesting entity.
- Unauthorized or unverifiable requests will be denied, and the requester will be notified of the reason for denial.

3. Investigation and Response

- Once a request is verified, ComData Solutions, Inc. will promptly investigate the call(s) in question by:
 - Identifying the source of the call within its network.
 - Reviewing call detail records (CDRs) and other relevant data to trace the call path.
 - Determining whether the call originated from a customer, a reseller, or an upstream/downstream carrier.
- A response will be provided within the required timeframe, typically no later than 24-48 hours, unless otherwise specified by the requesting entity.

4. Customer Notification and Action

- If the investigation determines that a customer of ComData Solutions, Inc. is responsible for the call(s) in question:
 - The customer will be notified immediately and required to cease any unlawful activity.
 - The customer's account may be suspended or terminated in accordance with the service agreement and applicable laws.
- If a reseller or carrier partner is involved, ComData Solutions, Inc. will notify the partner and work collaboratively to address the issue.

5. Record Keeping

- ComData Solutions, Inc. will maintain records of all traceback requests and responses for a minimum of two years.
- Records will include:
 - Details of the traceback request.
 - Results of the investigation.
 - Actions taken to address the issue.

6. Collaboration with Law Enforcement

- In cases where illegal robocalling activity is confirmed, ComData Solutions, Inc. will cooperate fully with law enforcement agencies by providing requested information and assistance in their investigations.

Prohibited Activities

- ComData Solutions, Inc. strictly prohibits the use of its network for illegal robocalling activities. Customers found engaging in such activities will face immediate account suspension or termination and potential legal action.
 - Employees or contractors who fail to comply with this policy or who obstruct traceback investigations will be subject to disciplinary action, up to and including termination.
-

Review and Updates

- This policy will be reviewed annually or as required by changes in regulatory requirements or industry standards.
 - Updates to the policy will be communicated to all relevant personnel, and training will be provided as needed to ensure compliance.
-

Approved by
Johnny Kincanon
President
Date: 12/15/2025

This **Traceback Request Policy** ensures that **ComData Solutions, Inc.** maintains its commitment to combating illegal robocalling and supporting industry and regulatory efforts to identify and mitigate unlawful call traffic.

