

SIPTREK LLC

RMP

Robocall Mitigation Database Plan for SIPTREK

1. Introduction

SIPTREK is committed to preventing and mitigating robocall activities. This document outlines the strategy for building and maintaining a Robocall Mitigation Database that will support compliance with relevant regulations such as the TRACED Act (Telephone Robocall Abuse Criminal Enforcement and Deterrence Act) and the FCC's rules on robocall mitigation.

2. Objectives

- **Ensure Compliance:** Adhere to regulations set forth by the Federal Communications Commission (FCC) regarding robocall mitigation.
 - **Improve Call Quality:** Enhance customer experience by reducing or eliminating spam, illegal robocalls, and scam calls.
 - **Transparency and Accountability:** Provide customers and regulatory bodies with data showing SIPTREK's commitment to mitigating robocalls.
 - **Improve Caller Identification:** Ensure that legitimate callers are properly identified, helping prevent fraud and improving trust in the telecommunications ecosystem.
-

3. Database Structure

The Robocall Mitigation Database will consist of several key components designed to track and manage information related to both SIPTREK's legitimate calls and any robocall mitigation efforts.

Database Components:

1. Caller ID Database:

- **Purpose:** Store valid, verified caller IDs associated with SIPTREK customers and partners.
- **Fields:**

-
- **Caller Name**
 - **Caller ID (Phone Number)**
 - **Verification Status** (Verified/Unverified)
 - **Company Name** (If applicable)
 - **Verification Date**
 - **Compliance Certification** (Yes/No)
2. **Robocall Mitigation Report:**
- **Purpose:** Track the details of robocall mitigation efforts, including registrations and certifications.
 - **Fields:**
 - **Caller ID**
 - **Date Registered**
 - **Mitigation Measures** (STIR/SHAKEN, Call Blocking, etc.)
 - **Certification Status** (Compliant/Non-Compliant)
 - **Record of Calls Blocked**
 - **Data of First Incident** (if applicable)
3. **Caller Authentication Logs:**
- **Purpose:** Store logs of authenticated calls that use caller ID verification protocols such as STIR/SHAKEN.
 - **Fields:**
 - **Call Start Time**
 - **Caller ID**
 - **Authentication Status** (Verified, Failed, Unknown)
 - **Authentication Protocol Used** (STIR, SHAKEN, etc.)
4. **Customer Feedback Database:**
- **Purpose:** Track customer reports of suspected robocalls, as well as responses to SIPTREK's mitigation measures.
 - **Fields:**
 - **Customer ID**
 - **Suspected Robocall Number**
 - **Date of Call**
 - **Type of Call** (Spam, Scam, Legitimate)
 - **Customer Action Taken** (Reported, Blocked, etc.)

4. Data Collection Methods

- **Verification of Caller IDs:** Every customer and partner will be required to submit proof of their identity for the purposes of call verification. This data will be stored in the Caller ID Database.

-
- **Third-Party Databases:** SIPTREK will subscribe to third-party robocall mitigation and call authentication services (e.g., SHAKEN/STIR service providers) to enhance the accuracy of the database.
 - **Customer Reports:** SIPTREK will collect reports from customers regarding suspected robocalls and integrate these reports into the Customer Feedback Database for analysis and response.
-

5. Database Management

- **Data Integrity:** Ensure the database is regularly updated with current data to reflect caller ID verification status and mitigation measures taken. Use automated systems to flag outdated or incomplete records.
 - **Access Control:** Limit access to sensitive data based on roles (e.g., network administrator, compliance officer). Implement multi-factor authentication (MFA) for administrative access.
 - **Backup and Recovery:** The database will be backed up regularly to ensure business continuity. Backup procedures will be tested annually to confirm their reliability.
-

6. Mitigation Measures

SIPTREK will implement the following measures to mitigate robocalls:

1. STIR/SHAKEN Implementation:

- SIPTREK will implement the STIR/SHAKEN protocol to authenticate outbound calls and block fraudulent calls.

2. Call Blocking:

- SIPTREK will block calls that originate from numbers deemed to be high risk for robocalls, based on data from trusted third-party sources and internal reports.

3. Whitelisting:

- SIPTREK will whitelist trusted businesses and organizations to ensure their calls are not inadvertently blocked, even if their numbers have been reported for robocalls.

4. Customer Opt-In Services:

- Provide SIPTREK customers with the option to opt-in for additional call blocking or call
- 

screening services, which can be configured via the customer portal.

7. Compliance with FCC Regulations

- **Robocall Mitigation Certification:**
 - SIPTREK will submit its robocall mitigation certification to the FCC, confirming compliance with STIR/SHAKEN standards and any other applicable rules.
 - **Annual Reporting:**
 - SIPTREK will maintain an annual report documenting the efforts taken to mitigate robocalls, the status of caller ID authentication, and any issues encountered during the mitigation process.
 - **Audits and Inspections:**
 - Conduct internal audits of the Robocall Mitigation Database to ensure that data is accurate and up to date. External audits will be requested if required by the regulatory authorities.
-

8. Monitoring and Enforcement

- **Real-Time Monitoring:**
 - Use real-time monitoring tools to track and analyze the effectiveness of call blocking and authentication efforts.
 - **Proactive Blocking:**
 - Automatically flag and block known robocall numbers as part of a real-time strategy.
 - **Customer Alerts:**
 - Notify customers about the status of their calls, including authentication failures or blocked calls, via SMS or email.
-

9. Reporting and Transparency

- **Transparency Dashboard:**
 - Provide stakeholders with access to an online dashboard that shows SIPTREK's current compliance status, number of calls blocked, and other relevant metrics.
 - **Incident Reports:**
 - If a serious robocall incident is detected, SIPTREK will produce a report detailing the
- 

situation, the response actions taken, and the steps implemented to prevent recurrence.

10. Conclusion

SIPTREK's Robocall Mitigation Database Plan will be a critical component of our overall strategy to combat robocalls and ensure that all outbound calls meet the highest standards of security and compliance. By taking proactive measures and maintaining an up-to-date and transparent database, SIPTREK aims to protect customers, enhance trust, and maintain a robust communications environment.