

CleveroTel Robocall Mitigation Plan

Prepared by: Mujeeb Rahman

Date: 20/12/2024

1. Introduction

This Robocall Mitigation Plan (RMP) outlines CleveroTel's measures to detect, prevent, and respond to illegal robocalls originating from or transiting through our network. This plan is designed to comply with applicable regulatory requirements, including FCC rules.

2. Company Information

- **Legal Entity Name:** Clevero Inc d.b.a CleveroTel
- **Primary Business Address:** 6495 Shiloh Rd, Ste 220, Alpharetta, GA 30005
- **Point of Contact for Robocall Mitigation:**
 - Name: Mujeeb Rahman
 - Title: Chief Technology Officer
 - Email: mujeeb@clevero.com
 - Phone: +1 6788843388

3. Overview of CleveroTel Network and Services

Network Infrastructure: CleveroTel's IP PBX network infrastructure is designed to deliver efficient, scalable, and secure voice communication solutions for enterprise and consumer needs. By leveraging modern IP-based technologies, the infrastructure supports seamless call management, robust security, and high-quality voice services. For best performance and best service delivery, we provide service through FreeSWITCH

FreeSWITCH is an open-source telecommunications platform designed for building communication systems such as Voice over IP (VoIP), video, and chat services. It's highly versatile and scalable, making it an ideal solution for both small businesses and large enterprises looking to manage their telephony needs. Below is a brief overview of **FreeSWITCH** and its key features, which could be relevant for implementing a **Robocal Mitigation Plan** for CleveroTel's IP PBX system. (**Appendix A**)

Key Features of FreeSWITCH Relevant for Robocall Mitigation

- **Call Routing and Filtering:**
 - **Call Control:** FreeSWITCH allows for advanced call routing based on specific rules, which could be configured to filter or block suspicious calls.
 - **Blacklist and Whitelist:** You can set up blacklist and whitelist rules for known robocall numbers or trusted sources. This feature would be particularly

useful for blocking known malicious callers or preventing automated systems from accessing the platform.

- **Dynamic Call Handling:** FreeSWITCH supports dynamic routing based on factors like time of day, call frequency, or call patterns, enabling more granular control over how calls are processed.
- **STIR/SHAKEN Support:**
 - **STIR/SHAKEN Integration:** FreeSWITCH can be configured to support STIR/SHAKEN protocols, which authenticate the identity of incoming calls to verify whether they are legitimate or spoofed. This integration would be vital for preventing robocalls and caller ID spoofing, a common tactic used by fraudsters.
- **IVR Systems:**
 - **Interactive Voice Response (IVR):** FreeSWITCH can be used to implement sophisticated IVR systems to challenge suspicious calls. Automated systems or robocalls often fail to interact with IVR systems that require responses or inputs from the caller.
 - **CAPTCHA Integration:** FreeSWITCH supports the integration of CAPTCHA-like mechanisms, where calls from automated systems might be presented with a challenge to verify they are human.
- **Call Analytics and Monitoring:**
 - **Real-Time Call Analytics:** FreeSWITCH provides tools for monitoring call traffic and detecting patterns typical of robocalls, such as high-frequency calling from the same number or geographic region. This can help identify fraud attempts early and implement real-time call filtering.
 - **Call Detail Records (CDRs):** FreeSWITCH generates detailed logs of all calls made through the system. These logs can be used for post-incident analysis and to identify abnormal patterns that could signal robocall activity.
- **Multi-Tenant Support:**
 - **Tenant Segmentation:** For a business like Cleverotel, which may have multiple hotel locations or departments, FreeSWITCH's multi-tenant capabilities allow for separate configurations and security measures for each department or hotel, making it easier to manage robocall mitigation on a per-tenant basis.
- **Voice Biometrics:**
 - **Biometric Authentication:** FreeSWITCH can be integrated with third-party voice biometric systems to provide additional layers of verification for sensitive calls, such as those related to reservations or payment details, ensuring that robocalls cannot impersonate legitimate customers.

Implementing Robocall Mitigation with FreeSWITCH

To mitigate robocalls using FreeSWITCH, CleveroTel could implement the following strategies:

- **STIR/SHAKEN Implementation:**
 - FreeSWITCH should be configured to work with STIR/SHAKEN to authenticate incoming calls, ensuring that any calls that appear to be spoofed or from an unverified source are blocked or flagged for further investigation.
- **Robocall Filtering:**
 - Utilize FreeSWITCH's call routing and filtering rules to block known robocall numbers, apply dynamic filtering based on patterns or time of day, and route

suspicious calls to an automated IVR that challenges the caller for more information.

- **Call Pattern Analysis:**
 - Implement real-time monitoring of call patterns using FreeSWITCH's call analytics tools. This can help identify unusual activity, such as an abnormal volume of calls from a particular number or region, which is common in robocall campaigns.
- **IVR and CAPTCHA:**
 - Use FreeSWITCH's IVR system to ask robocallers questions or request actions that require human interaction. Additionally, implementing a CAPTCHA system on the IVR for high-risk interactions (like making reservations or processing payments) can prevent automated systems from bypassing the filters.
- **Blacklist and Whitelist:**
 - Maintain an up-to-date list of blacklisted robocall numbers and trusted numbers in FreeSWITCH's configuration. Calls from blacklisted numbers should be automatically blocked, while calls from whitelisted sources are always allowed to pass through.
- **Integration with Third-Party Robocall Blocking Services:**
 - FreeSWITCH can be integrated with external robocall-blocking services, such as **Nomorobo**, **Hiya**, or **YouMail**, to augment its built-in call filtering capabilities. These services use databases of known robocallers to filter out suspicious calls before they reach the PBX system.

FusionPBX as Management Interface

FusionPBX acts as the front-end to FreeSWITCH, allowing users to set up and manage **(Appendix B)**:

- Extensions and user accounts
- Call routing (dial plans)
- Voicemail and voicemail groups
- Conferences and bridges
- Monitoring call stats and logs
- Security settings, including SIP password protection and firewall configuration

FusionPBX for Robocall Mitigation

Since FusionPBX is built on FreeSWITCH, it can be utilized to implement various **robocall mitigation strategies**. Below are some approaches to combat robocalls using FusionPBX:

A. Call Authentication and STIR/SHAKEN Implementation

- **STIR/SHAKEN** (Secure Telephone Identity Revisited and Signature-based Handling of Asserted information using Tokens) is a framework for authenticating caller IDs to prevent spoofing. FusionPBX, using FreeSWITCH, can integrate with STIR/SHAKEN to ensure calls are authenticated before reaching their destination. This helps in blocking robocalls that use fake caller IDs to disguise their true source.
- **Configuration:** The integration typically requires:

- Ensuring that the **SIP trunk providers** and **FreeSWITCH** support STIR/SHAKEN.
- Modifying the dialplan and authentication scripts within FusionPBX to validate and handle the **authentication tokens** from the STIR/SHAKEN protocol.
- Working with SIP providers or telecom operators who have STIR/SHAKEN compliance in place.

B. Call Blocking and Filtering

- **Blacklist and Whitelist:**
 - FusionPBX allows administrators to create **blacklists** for known fraudulent numbers or **whitelists** for trusted callers.
 - Automated systems can filter out calls from numbers that are commonly used for robocalling, based on known fraud patterns or suspicious activity.
- **Advanced Call Routing:**
 - Using FusionPBX's **dial plans**, admins can implement custom routing rules to block calls originating from certain regions or numbers that are typically associated with robocalls.
 - Calls can be routed through voice filtering systems, or even to an IVR system that requests additional verification before proceeding with the call.
- **Real-Time Call Monitoring:**
 - FusionPBX supports **real-time call monitoring** and can be set up to detect unusual patterns in call traffic, such as a large number of calls from the same number or location in a short period, which can often indicate robocall activity.

C. Integration with External Anti-Robocall Solutions

- **Third-Party Services:**
 - FusionPBX can be integrated with external robocall blocking services, such as **Nomorobo** or **Hiya**, using their APIs or by routing calls through their systems for additional verification.
- **Robocall Detection Algorithms:**
 - Advanced robocall detection can be implemented by leveraging machine learning models or **AI-powered tools** to analyze call patterns and identify robocall signatures. FusionPBX can use APIs to integrate with these services, ensuring more accurate filtering and blocking.

D. Automated Blocking of Unauthenticated Calls

- FusionPBX can automatically block calls that fail to meet certain criteria, such as not passing authentication checks or originating from suspicious regions. These calls can either be dropped entirely or sent to a **quarantine system** for further analysis.

3. Security Features in FusionPBX

To reduce the risk of robocalls and other malicious activity, FusionPBX comes with several security features:

- **IP-based Access Control:**
 - Restrict incoming and outgoing calls based on IP addresses or subnets, limiting access to trusted networks only.
- **SIP Password Protection:**
 - Ensure that all SIP accounts are protected with strong, complex passwords to prevent unauthorized access.
- **Rate Limiting:**
 - Implement rate limits to prevent large volumes of calls from being placed from a single source in a short amount of time, which is often a sign of robocalling activity.
- **TLS and SRTP Support:**
 - Use **TLS** (Transport Layer Security) for encrypted signalling and **SRTP** (Secure Real-Time Transport Protocol) for encrypted media, which prevents call interception and spoofing attempts.
- **Event Logging:**
 - FusionPBX can log all events and provide administrators with detailed logs of call activity, which is useful for detecting anomalous behaviour and potential fraud.

4. Reporting and Analytics in FusionPBX

- **Call Detail Records (CDR):**
 - FusionPBX provides detailed **Call Detail Records** (CDRs) that can be used to track all calls, including those originating from suspicious numbers.
 - Administrators can use these records to analyse patterns, detect robocalls, and generate custom reports.
- **Alerts and Notifications:**
 - FusionPBX can be set up to send real-time alerts for suspected robocall activity, such as a high volume of calls from a specific number or area code. This enables quick intervention and action.
- **Analytics Dashboard:**
 - The web interface provides analytics dashboards where call volume, call success rates, and call types (e.g., answered, failed, blocked) can be visualized to detect potential robocall issues.

CleveroTel Services Overview

CleveroTel is a comprehensive telecommunications provider offering a wide range of services designed to meet the needs of businesses, enterprises, and individual users. Its

offerings focus on delivering high-quality voice communication, robust connectivity, and value-added solutions to enhance productivity and efficiency.

1. Voice Services

- **Hosted PBX Services:**
 - Cloud-based PBX solutions with advanced call routing, voicemail, and IVR functionalities.
 - Fully managed and scalable for businesses of all sizes.
- **VoIP Services:**
 - High-definition voice calling over the internet for cost-effective communication.
 - Features include call forwarding, voicemail-to-email, and conference calling.
- **SIP Trunking:**
 - Enables businesses to connect their existing PBX systems to the PSTN via SIP-based trunking.
 - Scalable channels for simultaneous calls and reduced telecommunication costs.
- **International and Toll-Free Calling:**
 - Affordable international call plans with transparent pricing.
 - Toll-free numbers for businesses to enhance customer accessibility.

2. Unified Communications and Collaboration (UCaaS)

- **Video Conferencing:**
 - High-definition video and audio conferencing with screen sharing and collaboration tools.
- **Team Messaging:**
 - Real-time messaging with file sharing and team chat capabilities.
- **Integration with Business Applications:**
 - Seamless integration with CRM, ERP, and other enterprise tools.

3. Connectivity Services

- **Internet Services:**
 - High-speed broadband and fiber-optic connectivity for businesses and homes.
 - Dedicated leased lines for uninterrupted, reliable internet access.
- **VPN Solutions:**
 - Secure and private networks for remote workforce connectivity.

4. Security and Compliance Solutions

- **Robocall Mitigation Services:**
 - Tools and systems to block illegal robocalls and ensure compliance with FCC regulations.
- **Caller ID Authentication (STIR/SHAKEN):**
 - Protects against caller ID spoofing and enhances trust in communication.
- **Fraud Prevention Tools:**
 - Real-time monitoring and alerts for suspicious call activities.

5. Contact Center Solutions

- **Omnichannel Contact Center:**
 - Integrates voice, email, chat, and social media for a unified customer experience.
- **Call Recording and Analytics:**
 - Record and analyse calls to improve customer service and operational efficiency.
- **Interactive Voice Response (IVR):**
 - Automated IVR systems for efficient call routing and customer self-service options.

6. Managed Services

- **Network Monitoring and Management:**
 - Proactive monitoring to ensure uptime and performance.
- **Cloud Migration Support:**
 - Assistance in migrating traditional communication systems to the cloud.
- **Customized Solutions:**
 - Tailored telecommunication solutions to meet specific business requirements.

7. Additional Services

- **Emergency Services (E911):**
 - Enhanced 911 service for accurate location reporting in emergencies.
- **Mobile VoIP:**
 - Mobile apps to enable on-the-go connectivity with enterprise communication systems.
- **Number Porting:**
 - Hassle-free transfer of existing phone numbers to CleveroTel's network.

Target Customers

- **Small and Medium Businesses (SMBs):**
 - Affordable, scalable solutions tailored for growing businesses.
- **Large Enterprises:**
 - Robust and secure communication systems for enterprise-grade reliability.
- **Residential Customers:**
 - High-speed internet and VoIP services for personal use.

4. Robocall Mitigation Measures

4.1. Customer Vetting and Verification (Know Your Customer - KYC)

- Require detailed customer registration information (e.g., legal entity, address, contact info).
- Verify customer identity using trusted sources (e.g., government ID, business registration).
- Prohibit high-risk or suspicious customers from accessing services: Reject customers who cannot provide accurate or verifiable details.

4.2. CleveroTel Network Monitoring and Call Analytics

Overview:

CleveroTel employs advanced network monitoring and call analytics solutions to ensure the reliability, security, and efficiency of its telecommunications network. These systems enable real-time visibility into network performance, proactive issue resolution, and enhanced customer experience.

Key Features:

1. Network Monitoring

- **Real-Time Insights:**
 - Continuous tracking of network performance metrics, such as latency, jitter, packet loss, and bandwidth utilization.
 - Monitoring of voice quality using MOS (Mean Opinion Score) to ensure high call quality.
- **Fault Detection and Resolution:**
 - Automatic detection of network anomalies, outages, or congestion.
 - Proactive alerts for faster troubleshooting and minimized downtime.
- **Security Monitoring:**
 - Intrusion detection systems to identify and block unauthorized access or SIP-based attacks (e.g., DDoS, toll fraud).
 - Monitoring for compliance with regulatory standards like STIR/SHAKEN and robocall mitigation protocols.

2. Call Analytics

- **Call Traffic Analysis:**
 - Monitoring call volumes, durations, and peak traffic patterns to optimize resource allocation.
 - Identification of abnormal traffic patterns indicative of fraudulent or spam activity.
- **Quality of Service (QoS) Metrics:**
 - Detailed reports on call quality to identify and address issues affecting user experience.
- **Call Behaviour Analysis:**
 - Tracking dropped calls, call success rates, and abandoned calls to improve service delivery.
- **Fraud Detection and Prevention:**
 - Analytics to detect patterns of suspicious activity, such as call spoofing or mass dialling.
 - Blocking of flagged numbers and high-risk traffic.

Benefits:

1. **Operational Efficiency:**
 - Improved network reliability through proactive maintenance.
2. **Enhanced User Experience:**
 - Consistently high-quality communication services.
3. **Fraud Mitigation:**
 - Prevention of illegal robocalls and fraud, safeguarding customer trust.
4. **Scalability:**
 - Ability to adapt to changing traffic demands and business growth.

4.3. Call Authentication

Call authentication is a process used to verify the identity of the person making or receiving a phone call, ensuring that the call is legitimate and not fraudulent. This is especially important in the context of protecting sensitive information, preventing identity theft, and safeguarding against various types of fraud, such as social engineering attacks. There are several methods of call authentication:

1. **Caller ID Verification:** The most basic form of call authentication. The system checks if the caller's phone number matches the expected number (e.g., for a bank or service provider).
2. **One-Time Passwords (OTP):** A system sends a unique code to the user's phone, which must be entered during the call to authenticate the person.
3. **Biometric Verification:** Some systems use voice recognition or other biometric data to confirm the identity of the caller. Voice biometrics analyse speech patterns, tone, and other vocal characteristics.
4. **Call Blocking or Labelling Services:** These services use algorithms to detect robocalls or spoofed calls, reducing the likelihood of fraudulent calls reaching the

user. Some services label calls as “Spam” or “Potential Fraud” based on known patterns.

5. **STIR/SHAKEN Technology:** This is a standard for preventing call spoofing in the telecom industry. It authenticates calls at the network level to ensure that the caller’s identity matches the information provided by their carrier.

These methods help to improve security, particularly in industries such as banking, healthcare, and customer service, where sensitive data is exchanged over the phone.

4.4. Response to Traceback Requests

A "Traceback" in the context of programming refers to an error report that provides a detailed path of function calls, lines of code, and exceptions that led to a program crash or error. When a traceback is encountered, it's essential to carefully analyse it to diagnose the issue and find a solution.

- Commit to responding to traceback requests within 24 hours.
- Maintain detailed logs of call traffic for traceback purposes.

4.5. Blocking and Filtering of Illegal Traffic

Blocking and filtering of illegal traffic is a critical aspect of network security aimed at preventing unauthorized, malicious, or harmful traffic from entering or leaving a network. This is done to protect systems from attacks, fraud, data breaches, and other security threats.

- Use real-time filtering tools to block calls originating from known bad actors.
- Regularly update blocked-number lists based on intelligence and regulatory advisories.

5. Employee Training and Awareness at CleveroTel

Employee training and awareness are crucial components in the **CleveroTel Robocall Mitigation Plan**. Ensuring that staff are properly equipped with the knowledge and skills to recognize, handle, and respond to robocalls and fraud attempts can help protect the organization and its guests from potential threats. A well-educated team not only enhances security but also improves overall customer service and operational efficiency.

- Train employees to recognize and mitigate illegal robocall risks.
- Conduct regular reviews of policies and practices to ensure compliance.

6. Reporting and Compliance

In the context of **CleveroTel's Robocall Mitigation Plan**, **Reporting and Compliance** are crucial to ensure that the organization adheres to industry standards, regulatory requirements, and internal policies while also staying accountable for its efforts to combat robocalls and fraud. Proper reporting and compliance mechanisms also help to track the effectiveness of

mitigation efforts, identify areas for improvement, and ensure that the company's telephony system remains secure and trusted by guests and partners.

- Certify this plan with the FCC's Robocall Mitigation Database.
- Submit updates to the FCC whenever significant changes are made to this plan.

7. Ongoing Evaluation and Updates for Robocall Mitigation

The dynamic nature of robocall tactics, telecom fraud, and regulatory requirements necessitates continuous evaluation and updates to CleveroTel's robocall mitigation strategies. Ongoing evaluation ensures that the organization remains proactive in responding to emerging threats, adjusts its approaches based on real-world data, and stays compliant with evolving laws and industry best practices.

- Conduct quarterly reviews of the effectiveness of robocall mitigation measures.
- Update the RMP as necessary to address new threats or changes in regulations.

8. Contact Information for Escalation

- For inquiries related to this RMP, contact:
 - Name: Mujeeb Rahman
 - Title: Chief Technology Officer
 - Email: mujeeb@clevero.com
 - Phone: +1 6788843388

Acknowledgment

This Robocall Mitigation Plan has been reviewed and approved by CleveroTel's management.

Authorized Signatory:

Name: Geoffrey Thomas

Title: Product Manager

Signature:

Date:

Appendix A

FreeSwitch Specifications

- **Architecture:**
 - Modular, event-driven architecture.
 - Extensible through custom modules written in **C**, **Lua**, or **JavaScript**.
- **Supported Protocols:**
 - **SIP** (Session Initiation Protocol)
 - **WebRTC** (for browser-based communication)
 - **XMPP** (Extensible Messaging and Presence Protocol)
 - **H.323** (for legacy PBX systems)
 - **MGCP** (Media Gateway Control Protocol)
 - **IAX** (Inter-Asterisk eXchange)
- **Media Formats Supported:**
 - **Audio:** **G.711**, **G.729**, **G.722**, **Opus**, **iLBC**, **Speex**, and more.
 - **Video:** **H.264**, **VP8**, and **WebRTC** compatible video codecs.
- **Operating Systems:**
 - **Linux** (Ubuntu, CentOS, Debian, Fedora, etc.)
 - **Windows**
 - **macOS**

- **FreeBSD**
- **Scalability:**
 - Supports **high availability** and **load balancing** through clustering and multi-server deployments.
 - **Horizontal scaling** for large installations.
- **Database Support:**
 - FreeSWITCH can use **SQLite**, **MySQL**, or **PostgreSQL** for storing configuration data, logs, and CDRs.

FreeSwitch Security Features

- **SIP Authentication:**
Ensures that only authorized users can make calls.
- **Encryption:**
 - **TLS** for encrypted signalling.
 - **SRTP** for encrypted media streams, ensuring confidentiality.
- **Firewalling:**
FreeSWITCH includes configuration tools to control access based on IP address, making it possible to secure the server from unauthorized access.
- **Anti-Fraud Tools:**
Rate-limiting and call blocking prevent abuse and fraudulent activity such as toll fraud.

Appendix B

Fusion PBX Specifications

- **Architecture:**
 - Based on FreeSWITCH's modular architecture, FusionPBX acts as a graphical front-end that interacts with FreeSWITCH's core functionality.
 - Written in **PHP**, with database support for **SQLite**, **MySQL**, or **PostgreSQL**.
- **Supported Protocols:**
 - **SIP** (Session Initiation Protocol)
 - **WebRTC** (for browser-based communications)
 - **XMPP** (Extensible Messaging and Presence Protocol)
 - **H.323** (for legacy PBX integration)
 - **IAX** (Inter-Asterisk eXchange)
- **Media Formats:**
 - **Audio:** **G.711**, **G.729**, **G.722**, **Opus**, **iLBC**, **Speex**, and others.
 - **Video:** **H.264**, **VP8**, WebRTC-compatible video codecs.
- **Operating Systems:**
 - **Linux** (Ubuntu, CentOS, Debian, Fedora, etc.)
 - **FreeBSD**
 - **macOS**
 - **Windows**

- **Database:**
 - **SQLite**, **MySQL**, or **PostgreSQL** (for managing configuration data and CDRs).
- **Scalability:**
 - FusionPBX supports **horizontal scaling** and **high availability** by utilizing FreeSWITCH's clustering and load balancing features.
 - It can handle **thousands of extensions** and **multiple tenants** on a single instance.

Fusion PBX Security Features

- **SIP Authentication:**

Ensures that only authorized users can register and make calls.
- **Encryption:**
 - **TLS** for encrypted SIP signalling.
 - **SRTP** for encrypted media (audio/video).
- **Firewalling:**

FusionPBX allows configuration of firewall rules to prevent unauthorized access, including **IP whitelisting** and **rate-limiting**.
- **Brute Force Protection:**

Features to protect against SIP password guessing attacks by blocking or delaying excessive failed login attempts.
- **Audit and Logging:**

FusionPBX generates extensive logs, including call detail records (CDRs), to help track usage, troubleshoot issues, and ensure security compliance.