



## **Robocall Mitigation Plan**

### **1. Understanding Robocalls**

Robocalls are automated phone calls made with the intent to deliver a pre-recorded message or connect the recipient to a live agent for fraudulent, deceptive, or unwanted purposes. They pose a significant nuisance and security risk to consumers and can damage the reputation of service providers. As a responsible service provider, Cyber Guardian Consulting Group, LLC acknowledges the importance of mitigating robocall activities.

### **2. Implementation Steps**

#### **2.1. Caller Authentication Measures**

Implement caller authentication measures such as Secure Telephony Identity Revisited (STIR) and Secure Handling of Asserted information using toKENs (SHAKEN) protocols. These protocols help validate the authenticity of caller identification information, thereby reducing the likelihood of spoofed calls.

#### **2.2. Call Blocking and Filtering**

Utilize call blocking and filtering mechanisms to prevent known robocall numbers from reaching customers' devices. Maintain an updated database of blacklisted numbers and continuously evaluate and add new numbers identified as sources of robocalls.

#### **2.3. User Reporting Mechanisms**

Empower customers with user-friendly reporting mechanisms to flag suspicious calls they receive. Implement a streamlined process for customers to report robocalls, enabling Cyber Guardian Consulting Group, LLC to investigate and take necessary actions promptly.

## **2.4. Regulatory Compliance**

Adhere to regulatory requirements set forth by organizations such as the Federal Communications Commission (FCC) and comply with legislation aimed at combating robocalls, such as the Telephone Consumer Protection Act (TCPA) and the TRACED Act. Stay informed about updates and changes to regulations to ensure continuous compliance.

## **2.5. Educating Customers**

Educate customers about robocall threats and provide guidance on recognizing and avoiding potential scams. Regularly communicate best practices for safeguarding personal information and staying vigilant against fraudulent calls.

## **3. Continuous Improvement**

### **3.1. Performance Monitoring**

Monitor the effectiveness of robocall mitigation measures through key performance indicators (KPIs) such as the number of blocked robocalls, customer satisfaction ratings, and regulatory compliance metrics. Analyze trends and adjust strategies accordingly to enhance effectiveness.

### **3.2. Collaboration and Information Sharing**

Collaborate with industry peers, regulatory bodies, and law enforcement agencies to share insights and intelligence on emerging robocall tactics and threats. Participate in forums and initiatives aimed at collectively addressing the robocall epidemic.

### **3.3. Technology Upgrades**

Stay abreast of advancements in robocall mitigation technology and consider periodic upgrades to enhance capabilities and stay ahead of evolving threats. Invest in research and development to explore innovative approaches to combatting robocalls effectively.