

KW Corporation's Robo Call Mitigation Plan

Based on FCC Requirements

Introduction

This document outlines KW Corporation's plan to mitigate robo calls based on the FCC requirements, which include:

- Implementation of STIR/SHAKEN caller ID authentication framework utilizing SANSAY
- Registering in the Robo Call Mitigation Database and filing a certification
- Implementing reasonable analytics and blocking solutions to prevent illegal and unwanted calls
- Cooperating with law enforcement and industry efforts to trace and stop robo callers
- Educating and informing our clients on how we are doing our part to stop and avoid robo calls
- Utilization of "Know your Customer"

Mitigation plan

- We have already deployed the necessary software and hardware components to support STIR/SHAKEN in our IP network, and we have tested the interoperability and functionality of the system with our partners and vendors (SANSAY, VoIP Carriers)
- We have established a secure connection with the Secure Telephone Identity Governance Authority (STI-GA), which oversees the administration and operation of the STIR/SHAKEN framework, and we have obtained the necessary certificates and credentials to participate in the system.
- We have configured our network to transmit and receive the STIR/SHAKEN authentication and verification information for all IP-based calls, and we have enabled the verification indicator on our customers' phones.
- We have implemented a monitoring and reporting system to track the performance and effectiveness of the STIR/SHAKEN system, and we have designated a point of contact for the FCC and other stakeholders to communicate any issues or concerns.
- We have completed the STIR/SHAKEN implementation certification form and submitted it to the FCC
- KW Corporation maintains very close and personable relationships with our client base that conforms to "know your customer" ethics.

Additional Details

- We have already registered in the database and provided our basic information, such as our name, address, phone number, email, and FCC Registration Number (FRN).
- We have implemented reasonable analytics and blocking solutions to identify and prevent illegal and unwanted calls from reaching our customers. These solutions include: using STIR/SHAKEN data, network-level blocking of invalid, unallocated, or unused numbers, customer-level blocking of specific numbers or categories of calls, and third-party services or applications that offer advanced call filtering and screening options.

- We will cooperate with law enforcement and industry efforts to trace and stop robo callers, and we will participate in the Industry Traceback Group (ITG), which is a consortium of voice service providers that work together to identify the source and path of illegal or unwanted calls. We will also respond to requests for information or assistance from the FCC, the Federal Trade Commission (FTC), the Department of Justice (DOJ), and state attorneys general.
- We have educated and informed our customers about their rights and options to avoid robo calls, and we have provided them with clear and accessible information about our analytics and blocking solutions, our code of conduct and best practices, and the verification indicator. We have also advised them on how to report and file complaints about robo calls, and how to protect themselves from scams and fraud.
- We have completed the robo call mitigation program certification form and submitted it

Conclusion

We are committed to mitigating robo calls and protecting our customers from unwanted and illegal calls. We have implemented the FCC requirements for STIR/SHAKEN and the Robo Call Mitigation Database, and we have developed a comprehensive robo call mitigation program that covers all aspects of analytics, blocking, originating, tracing, and educating. We will continue to monitor and improve our program, and to cooperate with the FCC and other stakeholders to combat robo calls and enhance the security and integrity of the phone network.