

CASTLE CABLE ROBOCALL MITIGATION PROGRAM

Castle Cable does not have an obligation to implement STIR/SHAKEN because it lacks the facilities necessary to implement STIR/SHAKEN. Castle Cable does not meet the qualifications to obtain a SPC token. 47 CFR § 64.6304.

Castle Cable has contracted with a third-party carrier, Westelcom Networks to provide numbering for assignment to Castle Cable's customers as well as call routing of its customer's traffic. Castle Cable and Westelcom Networks connect via SIP. Westelcom Networks has fully implemented STIR/SHAKEN within its network and signs originating calls on behalf of Castle Cable's customers routing on the third-party's IP network.

Robocall Mitigation Program

All voice traffic that originates on Castle Cable's ("Castle Cable")'s network is subject to the following Robocall Mitigation Program.

Call Analytics

Westelcom Networks also provides robocall analytics and reputation scoring of Castle Cable's outbound traffic. Westelcom Networks utilizes ClearIP call analytics software by TransNexus, a third-party analytics vendor, to monitor all outbound voice traffic in real-time to prevent the origination or transit of illegal robocalls. The software provides detailed reporting to identify suspected illegal robocalls. The system alerts Westelcom Networks if it processes outbound calls where the calling number has a poor reputation or is invalid, unallocated, or on a Do Not Originate list. In turn, Westelcom Networks immediately notifies Castle Cable of any identified suspicious calls, originated by Castle Cable customers.

Investigation

Castle Cable investigates calls identified by Westelcom Networks as suspicious calls or those that have abnormal call volumes, patterns or activity consistent with illegal robocalls.

In addition, if Castle Cable has any other reason to suspect illegal robocalling or spoofing is taking place over its network, Castle Cable will work internally to identify the party that is using our network to originate, route, or terminate such calls and take appropriate action.

Enforcement

Illegal robocalls and fraudulent spoofing is prohibited on our network. If it is determined a Castle Cable customer is using our network to fraudulently spoof calls or to originate illegal robocalls, Castle Cable will either warn the customer to stop such practices or terminate their service as allowed per Castle Cable policy.

Know your Customer

Castle Cable has procedures in place to prevent new & renewing customers from using our network to originate illegal robocalls. Castle Cable thoroughly vets new residential and business customers by asking personally identifiable questions for additional security on each account before activating new service or making changes to existing services.

Residential customers are asked to provide their full name, address (physical and mailing, if different), last four digits of their social security number, date of birth, phone number, email, and establish a security question, and a password. Business customers are asked to provide their full name, address (physical and mailing, if different), phone number, email, and establish a security question, and a password. To initiate an account change, a customer must provide their password or the answer to their security question prior to initiating a change. If the customer is unable to provide that information the customer service representative will call the customer back using the number they provided at account setup.

Upstream Provider Knowledge

Castle Cable knows all the carriers from which it receives traffic and has confirmed that all of the carriers are listed in the Robocall Mitigation Database.

Castle Cable monitors all incoming traffic for suspicious call patterns indicative of illegal robocall activity. The connected carriers are made aware of any suspicious or illegal traffic and notified that, if the traffic does not cease, the calls may be blocked from entering Castle Cable's network.

Traceback

Castle Cable commits to cooperating with the Commission, law enforcement, and the industry traceback consortium in investigating and stopping any illegal robocallers that we learn are using our service to originate calls. Castle Cable commits to responding to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, within twenty-four (24) hours.

Robocall Mitigation Database Eligibility

Castle Cable has not, within the prior two years been involved in any recent, formal law enforcement or regulatory investigation into suspected unlawful robocalling.

Castle Cable has not been prohibited from filing in the Robocall Mitigation Database (RMD).