

Mid-Hudson Data Corp.
Mid-Hudson Cablevision, Inc.
Robocall Mitigation Plan SIP code 603+
Update April 2026

Mid-Hudson Data Corp. & Mid-Hudson Cablevision, Inc. (“Mid-Hudson”) has updated its voice network to comply with FCC's ongoing efforts to control illegal spam and fraud calls with the Eighth report and order that specifies that 603+ should be used to notify callers when calls are blocked using reasonable analytics.

To make sure that we comply with the FCC 25-15 we have updated our voice network so that anytime we block call calls using analytics we will pass 603+ along to notify the callers.

Here is what our responses will be like.

- The 603-status line uses the reason phrase "Network Blocked".
- The response contains a SIP reason header.

Mid-Hudson Data Corp.
Mid-Hudson Cablevision, Inc.
Robocall Mitigation Plan
Update February 2026

February 2, 2026

Mid-Hudson Data Corp. & Mid-Hudson Cablevision, Inc. (“Mid-Hudson”) have implemented the STIR/SHAKEN caller ID authentication framework rules in June of 2023 which furthered the FCC’s efforts to protect consumers against malicious caller ID “spoofing,” which is often used during robocall scam campaigns to trick consumers into answering their phones.

Mid-Hudson updated its network and STIR/SHAKEN caller ID authentication framework and uses public-key cryptography to securely transmit the information that the originating voice service provider knows about the identity of the caller and its relationship to the phone number it is using along with the call, allowing to terminate the information on the other end before it reaches its customers. Mid-Hudson utilizes TNS for Call Authentication Hub and STIR/SHAKEN.

Mid-Hudson updated its network infrastructure to enable it to authenticate and verify caller-ID information consistent with the framework. Mid-Hudson’s STIR/SHAKEN framework shares what it knows about the caller ID information transmitted with a call, that can be used to terminate, block or label illegal robocalls before those calls reach their subscribers.

Mid-Hudson Data Corp. Robocall Mitigation Plan

Mid-Hudson Data Corp. (“Mid-Hudson”) qualifies for the small provider extension of the deadline to implement STIR/SHAKEN call authentication and has adopted this robocall mitigation plan in accordance with the FCC’s rules to attempt to detect and limit the potential for the origination of unlawful robocalls on its network.

Subscriber Vetting

Mid-Hudson provides facilities-based wireline service to a customer’s premises physical premises and is therefore less vulnerable than other service providers to receipt of robocalls from customers that misrepresent their identity or location. Nonetheless, Mid-Hudson vets the identity of subscribers when (i) approving an application for service; (ii) provisioning of network connectivity; (iii) entering into a contract agreement; or (iv) granting the right-to-use telephone number resources. Mid-Hudson collects the customer’s legal name and address, physical location, contact information, and, for commercial customers, jurisdiction of incorporation, federal tax ID, and the nature of the customer’s business. Mid-Hudson will not provide service if a new customer’s identification cannot be verified.

Telephone Number Validation

Telephone calls originated by Mid-Hudson subscribers typically are associated only with telephone numbers assigned by, or ported to, Mid-Hudson or its service providers. If a subscriber transmits calls with a different telephone number in its Caller ID information, Mid-Hudson will seek to validate the customer’s right to use such telephone number.

Cooperation with the Traceback Group, Law Enforcement and Government Agencies

Mid-Hudson’s policy is to timely cooperate with valid requests made by the Industry Traceback Group (ITG), law enforcement authorities, and government agencies to investigate and address suspected unlawful robocalls originated or passed to Mid-Hudson by Mid-Hudson’s customers. Mid-Hudson has engaged in discussions with a representative of the ITG and provided the ITG with contact information for a dedicated point of contact. Mid-Hudson will endeavor to timely assist with investigating the source of suspicious traffic.

Ongoing Robocall Mitigation and Monitoring

Mid-Hudson has partnered with Transaction Network Services (TNS) to implement Call Guardian Authentication Hub to assist in identifying calling patterns that are indicative of caller ID spoofing or voluminous unlawful robocalling originating from Mid-Hudson’s end users or that are received for delivery to Mid-Hudson end users. Such indicia may include, but are not limited to:

- Reputation score of the calling party calculated by TNS based upon data from a variety of sources and analytics
- excessive short duration calls
- being the subject of an ITG, law enforcement or government inquiry, or consumer complaints
- determination that the originating caller does not own or is not authorized to use the Caller ID number, or that the Caller ID name does not match the customer’s corporate

- name, trademark, or d/b/a name; and
- calls that stop attempting to connect after a single ring.

Mid-Hudson will seek to identify any customer that is using its network to originate such calls and take appropriate action, which may include termination or service and/or notification to law enforcement authorities.