

STIR/SHAKEN IMPLEMENTATION & ROBOCALL MITIGATION PLAN (RMP)

(February 18, 2026 Update)

Pursuant to 47 C.F.R. § 64.6305, Virgin Islands Telephone Corporation d/b/a Viya, Vitelcom Cellular, Inc. d/b/a Viya Wireless, Innovative Long Distance d/b/a Viya Long Distance, and Choice Communications, LLC d/b/a Viya Choice (collectively, “Viya”) submit this report on its implementation of the STIR/SHAKEN call authentication framework and its plan to prevent and mitigate illegal robocalls, as of February 18, 2026. Viya reserves the right to modify, add, delete or otherwise alter any of the policies and procedures described in the plan at any time as it deems appropriate to reflect its business, its capabilities, and its needs.

Company Background

Viya is the incumbent local exchange carrier in the U.S. Virgin Islands, providing wireline telephone service and through its affiliates, mobile telephone, internet and cable TV services to residential and business customers. The economy of the U.S. Virgin Islands is dominated by tourism and small businesses. Although there are a handful of large enterprises, most are government offices or quasi-government entities such as the Water and Power Authority and there are no private businesses with more than 100 lines.

Viya is not, and really cannot be, a significant source of U.S. robocalls. Nevertheless, Viya has implemented a Robocall Mitigation Program for its entire operation and Viya has deployed protections designed to ensure that it remains free of illegal robocalls on its network.

STIR/SHAKEN Implementation

Viya will comply fully with all conditions set forth in the FCC’s orders, rules, and policies regarding the implementation of the STIR/SHAKEN framework including the First Call Authentication Report and Order and Second Call Authentication Report and Order.¹

Viya exchanges virtually all of its traffic on the non-IP portions of its network as our access and interconnection arrangements are TDM-based. Under the FCC’s rules, Viya is not required to implement STIR/SHAKEN for these calls at this time. However, as described below, Viya has implemented a Robocall Mitigation Plan for these and other calls it delivers over its network.

Robocall Mitigation Plan

This Robocall Mitigation Plan describes the specific measures that Viya has implemented to detect and prevent illegal robocalls on its network as of February 26, 2024. Viya is not a significant source of illegal robocalls at this time and has tailored its robocall mitigation practices to address the areas most at risk of involving illegal robocalls. The measures described below explain how Viya mitigates and addresses the risk it experiences. Viya will periodically evaluate

¹ *Call Authentication Trust Anchor; Implementation of TRACED Act Section 6(a)—Knowledge of Customers by Entities with Access to Numbering Resources*, WC Docket Nos. 17-97 and 20-67, Report and Order and Further Notice of Proposed Rulemaking, FCC 20-42 (rel. Mar. 31, 2020); *Call Authentication Trust Anchor*, WC Docket Nos. 17-97, Second Report and Order, FCC 20-42 (rel. Oct. 1, 2020).

the risks it faces, the effectiveness of its policies and procedures, and its capabilities to support the measures described. Should it determine that changes are appropriate, its practices may differ from those described below.

Customer Due Diligence

- Viya conducts a comprehensive due diligence and credit review before establishing a contractual relationship with customers and revisits such diligence upon contractual renewals. Viya requires business customers to provide a copy of their Virgin Islands Business License as well as their taxpayer identification number. Residential customers must provide identification as well as a physical address (no P.O. Box) and there are measures in place to prevent sales representatives from bypassing these requirements.
- Viya monitors all of its services for violations of its Acceptable Use Policy (AUP), including excessive use.
- Viya will terminate or suspend service to customers with a history of non-compliance with its contractual obligations, including provisions relating to acceptable use of the service.

Viya will prevent the origination of illegal robocalls on our voice network and assist with tracing and stopping illegal robocalls originating on other service providers. This is achieved through:

- **Contractual Provisions** – Viya tariffs, service agreements, and its Acceptable Use Policy prohibit unlawful uses of service and provide for suspension and/or disconnection for violations of these provisions. Subscribers have an obligation not to use the services for any unlawful purpose, not to engage in any fraudulent uses, and to cooperate with Viya in mitigating unlawful activities.
- **Robocall Monitoring** – Working with its affiliates, Viya utilizes an analytics-based monitoring system to detect robocalling originating or traversing its network. This system monitors all call attempts through the network each hour, 24 hours a day. Reports are generated for Viya's NOC to research anytime certain triggers are hit such as excessive short duration calls.
- **Preventing CLID "Spoofing"**. We will screen end subscriber lines to prevent the transmission of un-owned directory numbers on subscriber lines through Calling Line Id (CLID) screening.
 - Viya permits only the transmittal of customer owned directory numbers (DNs) as the Calling Line ID (CLID) for calls originating on Viya's network.
 - a. By default, subscribers cannot override the Viya caller ID presentation. The calling subscriber can block, but is unable to override number.

- i. For traditional POTS and VoIP subscriber lines, the CLID is assigned during the installation process and is either the DN assigned to the line or another DN on the same customer account.
 - ii. For VoIP SIP and ISDN PRI subscriber trunks, the CLID may be signaled by the customer's communication system (PBX). All numbers signaled by the customer's PBX are validated against the DID numbers assigned to the trunk on which the call is received by the Viya's central office (CO) equipment. If the customer signaled CLID does not match a DN assigned to the trunk, the call will be rejected or the customer's primary DN will be substituted (depends on CO equipment).
 - b. If a customer wishes to transmit a DN as their CLID that is not assigned to their account, they must present proof of ownership of the DN. In this case the CLID of the trunk will be statically assigned to this DN for all outbound calls on that trunk group and all other signaling from the customer PBX will be ignored by CO equipment. No pass through of un-owned DNs as CLID is permitted by the CO equipment.
- Viya blocks traffic from invalid numbers by default. Viya also will block traffic that appears to be illegal or is flagged as suspicious under its AUP

Responding to Traceback Requests

- Viya is committed to respond within 24 hours to all traceback requests from the Commission, law enforcement, and the industry traceback consortium, and to cooperate with such entities in investigating and stopping any illegal robocallers that use its service to originate calls.
- Viya maintains current and correct information about its upstream carrier customers so that it can provide accurate responses to traceback requests.
- Viya has the following measures in place if a customer violates Viya's AUP or is the subject of a traceback request:
 - A known violation of Viya's Acceptable Use Policy triggers a notice and inquiry to the customer requesting explanation for the violation and providing a warning that if the violation continues the customer will be subject to further action up to and including termination. Viya will work with the customer to identify the source of the violation and request certification that the customer has policies and procedures in place to prevent originating or exchanging illegal traffic.
 - If the customer is the subject of repeated AUP violations, Viya will conduct its own investigation and will place the customer's traffic under increased scrutiny until it is satisfied the illegal traffic has stopped.
 - If the customer has a third AUP violation, Viya will terminate the customer relationship and stop exchanging the customer's traffic.

- Viya maintains records of any traceback request it receives and the carrier customer involved in the request.

Cooperation with State and Federal Regulators

Viya will cooperate with state and federal regulators to prevent any and all illegal robocalls. Specifically, Viya will:

- Respond to request for information about illegal robocalls;
- Provide relevant non-proprietary information in response to reasonable and legitimate requests about illegal robocalls and suspicious activities; and
- Implement mandated robocall mitigation procedures to the fullest extent possible with the goal of maximizing the mitigation of illegal robocalls.

Do Not Originate

Pursuant to 28 U.S.C. § 1746, that the telephone number(s) referenced in my STIR/SHAKEN filing did not originate any of the calls associated with the unlawful, fraudulent, or otherwise unauthorized activity described in the accompanying complaint. Any call that appears to have originated from this number was made without the knowledge, consent, or authorization of the lawful subscriber and constitutes unlawful caller ID spoofing in violation of the Truth in Caller ID Act (47 U.S.C. § 227(e)) and the Federal Communications Commission's implementing rules at 47 C.F.R. § 64.1604.

Pursuant to FCC requirements governing caller ID authentication and robocall mitigation under the STIR/SHAKEN framework (47 C.F.R. § 64.6300 et seq.), I affirm that the legitimate subscriber or owner of the number did not place, direct, permit, authorize, or otherwise participate in any of the calls in question. Any such call traffic is the result of misuse by an unauthorized third party and is inconsistent with the obligations imposed on voice service providers to prevent illegal spoofing and unlawful call origination.

Viya's Acceptable Use Policy

Acceptable Use Policy

Viya Acceptable Use Policy

Viya offers its Customers and Users the means to acquire and disseminate information through the Internet and by use of Viya's mobile and fixed-line communications networks (the "Service"). Viya reserves the sole discretion to deny or restrict your Service, or immediately to suspend or terminate your Service, if the use of your Service by you or anyone using it, in our sole discretion, violates the Service Agreement or other Viya policies, is objectionable or unlawful, interferes with the functioning or use of the Internet or the Viya network by Viya or other users, or violates the terms of this Acceptable Use Policy ("AUP"). Customers and Users will not resell or redistribute, or enable others to resell or redistribute, access to the Service in any manner, including, but not limited to, through the use of wireless technology. Viya reserves the right to take the preventative or corrective actions to protect its network, Customers, and Users, as well as other Service users and systems, which are outlined in this AUP. This AUP, including the below list of Prohibited Uses, outlines certain terms to which Viya Customers and other users must adhere. By using a Viya Service you agree to comply with this AUP and the provision of Service to you by Viya is conditioned on your compliance with this AUP. Viya reserves the right to change or modify the terms of the AUP at any time, and use of the Service after changes to the AUP are posted shall constitute acceptance of any changed or additional terms.

Prohibited Uses

Viya prohibits its Customers and Users from any uses of the Service, and any activities involving the Service, that are illegal, infringe the rights of others, interfere with or diminish the use and enjoyment of the Service by others, or interfere or impede Viya's ability to manage the Service. Viya may determine at its sole discretion whether a particular use or activity is permissible. Any activity or use of the Service which violates system or network security or integrity are prohibited and may result in criminal and civil liability. Such violations include, without limitation, the following:

- Unauthorized access to or use of data, systems, or networks, including any attempt to probe, scan, or test the vulnerability of a system or network, or to breach security or authentication measures without express authorization of the owner of the system or network.
- Unauthorized monitoring of data or traffic on any network or system without express authorization of the owner or network;
- Interference with Internet service to any user, host, or network, including but not limited to: mail bombing, flooding, or denial of service attacks.
- Forging the header of any transmitted information packet, email, or Usenet posting;

- Modifying or tampering with any hardware, software, or configuration provided by Viya including but not limited to: routers, switches, computers, and cable modem configuration files.
- Reselling or otherwise redistributing the Service.
- Disrupting, degrading or otherwise adversely affecting Viya's network or computer equipment owned by Viya or other Viya subscribers.
- Excessive use of bandwidth that in Viya's sole opinion, places an unusually large burden on the network or goes above normal usage. Viya has the right to impose limits on excessive bandwidth consumption via any means available to Viya.
- Transmit unsolicited bulk or commercial messages commonly known as "spam" or, in the case of telephone calls, "robocalling."
- Assuming or assigning a Viya IP address that was not allocated to the user by Viya or its network - all Viya Internet users must use DHCP assigned by the Service to acquire an IP address.
- Either of the following activities by a Customer or User using dedicated machines (also known as "machines" or "dedicated servers" or "autodialers") or virtual dedicated servers (also known as "VDS", "VPS", "virtual machines", and/or "virtual servers"): (i) running a tunnel or proxy to a server at another host, (ii) hosting, storing, proxy, or use of a network testing utility or denial of service (DoS/DDoS) tool in any capacity, (iii) generating bulk messages or telephone calls through the use of autodialers; or (iv) falsifying the information transmitted to a caller ID display for the purposes of disguising identity.
- Distributing in any way information, software or other material obtained through the service or otherwise that is protected by copyright or other proprietary right, without obtaining any required permission of the owner
- IP address translation or similar facilities intended to provide additional access.
- Transmission, distribution or storage of any material in violation of any applicable law or regulation. This includes, without limitation, any material that infringes or misappropriates the intellectual property of others, including copyrights, trademarks, service marks, trade secrets, or other intellectual property used without proper authorization, and material that is obscene, defamatory, abusive, harassing, threatening, or violates export control laws, including but not limited to images containing child pornography.
- Subscribing email addresses to any mailing list without the consent of the email address owner, forging or misrepresenting message headers, whether in whole or in part, to mask the originator of the message, or impersonating any person or entity.
- Posting commercial messages to a USENET group without first receiving approval from that USENET group.

- Participating in the collection of very large numbers of email addresses, screen names, or other identifiers of others without their consent, or participating in the use of software to facilitate this activity, including spyware.
- Advertising, transmitting, or otherwise making available any software, program, product, or service that violates this AUP, which includes, but is not limited to, the facilitation of the means to send spam, Internet viruses, worms, Trojan horses, pinging, flooding, mail-bombing, or denial of service attacks.
- Accessing illegally, or without authorization and consent, computers, accounts, or networks belonging to another party, attempting to breach the security of another user or system, or attempting to circumvent the user authentication or security of any host, network, or account. This includes any activity that might be used as a precursor to such conduct, including a port scan, stealth scan, or other information gathering activity.
- Accessing, or attempting to access, through deception computers, accounts or networks belonging to another party. This includes the sending of emails or messages purporting to be from reputable entities in order to induce others to reveal personal information such as passwords and financial information (commonly referred to as “phishing”).
- Engaging in any activity for an unlawful purpose, including advertising, transmitting, or otherwise making available Ponzi schemes, pyramid schemes, fraudulently charging credit cards, and pirating software.

Your Responsibilities

You are responsible for any and all use or misuse of your Service, including by a friend, family member, guest, or other user with access to your Service account. You must therefore take steps to ensure that others do not use your account to gain unauthorized access to the Service by, for example, strictly maintaining the confidentiality of your Service user ID and password (“Credentials”). You agree to notify Viya immediately of any unauthorized use of your Service or Credentials, or any other breach of security applicable to the Service. You may not use anyone else’s Service or Credentials at any time without their prior approval.

How Viya Enforces this AUP

Viya reserves the sole discretion to deny or restrict your access to the Service, or immediately to suspend or terminate your Service, if the use of your Service by you or anyone else, in our sole discretion, violates the terms of (a) this AUP (b) any agreements Viya has with any of its service providers (c) other agreements you have with Viya ,including other Viya policies, or otherwise is objectionable or unlawful or interferes with the functioning or use of the Internet or the Viya network by Viya or other users.

For example, Viya may suspend traffic to and from your IP address, email, or phone number in the event of (a) a denial of service attack, (b) detection of a botnet, (c) propagation of computer viruses or other programs, (d) propagation of unsolicited bulk messages, (e) malicious and premeditated congestion of Viya’s network, (f) falsification of the identity of packages and messages (including modification of the heading of TCP/IP packages, electronic mail messages and message), or (g) other similar attacks on Viya’s network or customers. Viya also reserves the right to monitor and refuse to transmit or post, and to remove or block, any information or

materials, in whole or in part, that it, in its sole discretion, Viya deems to be in violation or otherwise inconsistent with this AUP. However, neither Viya nor any of its affiliates, suppliers, or agents have any obligation to monitor transmissions or postings made through the Service.

Viya reserves the right to investigate violations of this AUP, including the gathering of information from the Customer or other Users involved and the complaining party, if any, and the examination of material on Viya's servers and network. Viya prefers to advise Customers and Users of AUP violations and any necessary corrective action but, if Viya, in its sole discretion, determines that a Customer or User has violated the AUP, Viya will take any responsive action that is deemed appropriate without prior notification. Viya is not liable for any such responsive action and these actions are not exclusive. Viya may take any other legal or technical action it deems appropriate. The failure by Viya or its affiliates to enforce any provision of this Policy at any given point in time shall not be construed as a waiver of any right to do so at any future time thereafter.

Copyright Infringement and the Digital Millennium Copyright Act

Viya respects the intellectual property rights of third parties. Accordingly, Customers and Users may not store any material or use Viya's systems or servers in any manner that constitutes an infringement of third party intellectual property rights, including, for example, under copyright law. Pursuant to Section 512 of the Digital Millennium Copyright Act, it is Viya's policy to terminate the account of repeat copyright infringers in appropriate circumstances. In addition, Viya expressly reserves the right to suspend, terminate or take other interim action regarding the Service of any Customer or user if Viya, in its sole judgment, believes that circumstances relating to an infringement of third party intellectual property rights warrant such action. These policies are in addition to and do not affect or modify any other rights Viya may have under law or contract.

Effective Date
Viya reserves the right to amend this AUP effective upon posting to our website or delivery of a written notice to you.

Last updated June 3, 2021.

ATN International, Inc.

Freedom 3 Investments IV, LP

Alaska Communications Systems Holdings, Inc. ACS of Alaska, LLC

ACS of the Northland, LLC

ACS of Fairbanks, LLC

ACS of Anchorage, LLC

ACS Long Distance, LLC

Alaska Communications Internet, LLC

ACS Cable Systems, LLC

ACS Cape Newenham ES Acquisition, LLC

ACS Indian Mountain ES Acquisition, LLC

ACS of the Northland License Sub, LLC

ACS of Anchorage License Sub, LLC

ACS of Fairbanks License Sub, LLC

ACS Sparrevohn ES Acquisition, LLC

ACS Wireless License Sub, LLC

ACS Long Distance License Sub, LLC

Northstar License Corporation

Atlantic Teleconnection Operating Company Limited Bermuda Digital Communications Ltd.

Choice Communications LLC

Commnet AZ LLC

Commnet Four Corners LLC

Commnet of Arizona LLC

Commnet of Nevada LLC

Commnet of Nevada, Subco

Commnet Rural America, LLC

Commnet Wireless, LLC

EssexTel Inc.

Excomm LLC

GTT, Inc.

Innovative Long Distance, Inc.

Logic Communications Ltd.

Mora Valley Wireless LLP

NTUA Wireless, LLC

Sacred Wind Communications, Inc.

Sal Spectrum, LLC

SW DinehN et, LLC

SW Telesolutions, Inc.

Virgin Islands Telephone Corporation

VITELCOM Cellular Inc.

WestNet Nevada LLC

WestTel Limited

Entity Details: Name	Affiliation Details: Name	Affiliation Details: Role	Affiliation Details: Title
Bermuda Digital Communications Ltd.	Niall Sheehy	President	President
Bermuda Digital Communications Ltd.	Kimberley Caines	Secretary	Secretary
Bermuda Digital Communications Ltd.	Jeanene Patrice Stovell	Assistant Secretary	Assistant Secretary
Bermuda Digital Communications Ltd.	Mary M. Mabey	Assistant Secretary	Assistant Secretary
Cedar Cable Ltd.	Niall Sheehy	President	President
Cedar Cable Ltd.	Kimberley Caines	Secretary	Secretary
Cedar Cable Ltd.	Jeanene Patrice Stovell	Assistant Secretary	Assistant Secretary
Cedar Cable Ltd.	Mary M. Mabey	Assistant Secretary	Assistant Secretary
Commnet Wireless, LLC	Michele A. Satrowsky	Assistant Treasurer	Assistant Treasurer
Commnet Wireless, LLC	Brad W. Martin	President	President
Commnet Wireless, LLC	Mary M. Mabey	Assistant Secretary	Assistant Secretary
Commnet Wireless, LLC	Carlos Doglioli	Treasurer	Treasurer
Commnet Wireless, LLC	James Ellison	Assistant Treasurer	Assistant Treasurer
Commnet Wireless, LLC	Neo Nicolaou	General Manager	General Manager
EssexTel, Inc.	Edward Dement	President	President
EssexTel, Inc.	Richard Bosler	Other	Vice President, Carrier Services
EssexTel, Inc.	Mary M. Mabey	Secretary	Secretary
EssexTel, Inc.	Michele A. Satrowsky	Assistant Treasurer	Assistant Treasurer
EssexTel, Inc.	Carlos Doglioli	Treasurer	Treasurer
Logic Communications Ltd.	Kimberley Caines	Secretary	Secretary
Logic Communications Ltd.	Patrice Stovell	Assistant Secretary	Assistant Secretary
Logic Communications Ltd.	Mary M. Mabey	Secretary	Secretary
NTUA Wireless, LLC	Mary M. Mabey	Secretary	Secretary
NTUA Wireless, LLC	Velen Tsosie	Other	General Manager
Sacred Wind Communications, Inc.	Terry Clark	Assistant Treasurer	Assistant Treasurer
Sacred Wind Communications, Inc.	Michele A. Satrowsky	Assistant Treasurer	Assistant Treasurer
Sacred Wind Communications, Inc.	Andrew Fienberg	Assistant Treasurer	Assistant Treasurer
Sacred Wind Communications, Inc.	Brad W. Martin	President	President
Sacred Wind Communications, Inc.	Mary M. Mabey	Assistant Secretary	Assistant Secretary
Sacred Wind Communications, Inc.	Carlos Doglioli	Assistant Treasurer	Assistant Treasurer
Sacred Wind Communications, Inc.	Neo Nicolaou	General Manager	General Manager
SW DinehNet, LLC	Terry Clark	Assistant Treasurer	Assistant Treasurer
SW DinehNet, LLC	Michele A. Satrowsky	Assistant Treasurer	Assistant Treasurer
SW DinehNet, LLC	Andrew Fienberg	Assistant Treasurer	Assistant Treasurer
SW DinehNet, LLC	Brad W. Martin	President	President
SW DinehNet, LLC	Mary M. Mabey	Assistant Secretary	Assistant Secretary
SW DinehNet, LLC	Neo Nicolaou	General Manager	General Manager
Virgin Islands Telephone Corporation	Brad W. Martin	President	President
Virgin Islands Telephone Corporation	Michele A. Satrowsky	Assistant Treasurer	Assistant Treasurer
Virgin Islands Telephone Corporation	Domenic C. Micale	Assistant Treasurer	Assistant Treasurer
Virgin Islands Telephone Corporation	Carlos Doglioli	Treasurer	Treasurer
Virgin Islands Telephone Corporation	Paul Kouroupas	Secretary	Secretary
Virgin Islands Telephone Corporation	Mary M. Mabey	Assistant Secretary	Assistant Secretary
Virgin Islands Telephone Corporation	Siobhan James-Alexander	Chief Executive Officer	Chief Executive Officer
Virgin Islands Telephone Corporation	Darragh Dolan	Chief Financial Officer	Chief Financial Officer
WestTel Limited (d/b/a Logic)	Niall Sheehy	Vice-President	Vice-President
WestTel Limited (d/b/a Logic)	Mark Reynolds	Secretary	Secretary