

Poweredge Networking LLC Robocall Mitigation Plan. 2026



Measures we have in place to avoid originating illegal robocall traffic as part of our robocall mitigation program,

- Poweredge Networking LLC uses BULKVS (FRN 0022777379) as our main carrier to server(resell) our customer's DIDs.

- BULKVS (FRN 0022777379) has fully implemented Stir/shaken. Our Stir/Shaken is through them(our carrier) From them I quote an email in our records, on 04/05/2024:

Inbound calls to your system will have the Stir/Shaken headers, and outbound calls not signed prior will be signed by our system before hitting PSTN.

Support

---- on Wed, 03 Apr 2024 11:31:00 -0400

- Our PBX has the WAN IPs required by the carrier allowed in the firewall, for them to verify with our PBX.

- Poweredge Networking does not sell origination or termination services to subscribers outside of the United States.

- We pay the PBX license that includes GeoFirewall, Limiting access to other than USA registration or invites, and the BULKVS ones.

- We serve only local and state business but we will Not serve any Telemarketing company, to be signed in the service agreement.

- Inbound calls are using CNAM queries, Outbound calls are set with our customer CID, same as registered in the carrier and E911 address verification.

- Our PBX monitors the traffic. We also have a Zabbix Server monitoring the traffic in and out of the PBX, with alarm set to unusual traffic.

- Our customer doesn't have access to the PBX system configuration, they can NOT change their own CID.

Today our customer is less than 50 user, with planning to up to 300 this first year

- We limit the contacts allowed per subscriber in the PBX to the exact amount the customer uses, avoiding registrations in the PBX other than the subscriber.

- We have not been prohibited from filing a certification in the Robocall Mitigation Database.

- Poweredge Networking LLC has not nor any of us have a history of enforcement actions for illegal robocalls, TCPA or TSR violations or related state law violations.

- USAC, Our Universal Service Administrative Co, 499 ID: 836753

Know Your Customer: We follow the best practices for vetting caller identity described by the NANC Call Authentication Trust Anchor Working Group. (<https://docs.fcc.gov/public/attachments/DOC-367133A1.pdf>)

- PowerEdge Networking Will collaborate to respond 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.

- We are committed to respond to any request within 24 hours and provide information available for the requested call, adding our actions against the fault.

- All our CID are named as per the End users, business owners, who signed our service under contract. Can't be changed and must contain reference to the business name as a rule.

- Agreement with the END users to terminate service and for them to take full responsibility if fraudulent calls are made and their accounts must be terminated. Penalties must be the customer's liability. Below is a the agreement copy:

- Contacts in Poweredge Networking:

R. Martinez	owner	7862292790, 8884832794
A.Perez	Manager	7862292794

poweredgenet@pe-svc.com
poweredgenet@gmail.com

Robocall and Scam calls mitigation agreements. Account #:_____

At PowerEdge Networking LLC, we care about your safety and security, especially when it comes to phone calls and communications. We want to emphasize your role in preventing robocall and scam calls to protect yourself and your personal information.

1. Stay Informed: It's essential to stay informed about common scam call tactics and robocall threats. Awareness is your first line of defense against fraudulent calls. Familiarize yourself with the latest scams and be cautious when receiving unexpected calls or messages.

2. Caller ID Verification: Always verify the identity of the caller before sharing any personal or financial information. If a call seems suspicious, hang up and independently verify the caller's identity through our official contact information.

3. Do Not Share Personal Information: Never share sensitive personal information, such as Social Security numbers, bank account details, or credit card information, over the phone unless you are certain of the caller's legitimacy.

4. Report Suspicious Calls: If you receive a robocall or a suspicious call, report it to your phone service provider, and consider reporting it to the appropriate authorities, such as the Federal Trade Commission (FTC). Your reports can help identify and track down scammers.

5. Be Skeptical of Urgency and charity calls: Scammers often create a sense of urgency to pressure you into making quick decisions. Take your time, verify the situation, and consult with us if necessary.

6. Protect Your Personal Information: Safeguard your personal information and be cautious about sharing it online or in response to unsolicited calls or messages.

Remember that you have a vital role in preventing robocall and scam call incidents. By staying informed, practicing caution, and reporting suspicious activity, you contribute to a safer communication environment for yourself and others.

Making unauthorized calls such as Robocalls, scams, unsolicited sales, incurs federal crimes that must be reported to the FCC and other legal authorities. Incurring in this crime entails your total responsibility before the law, as well as your sole liability for charges, fees, and penalties that this may entail. If any of the aforementioned crimes occur, PowerEdge Networking LLC must cancel your service. Our company is not responsible for your misuse.

Cancellation of the service does not exempt the customer from paying any fees or services provided up to the time of cancellation.

Service Provider Signature_____

Client Signature_____

By: _____

By: _____

[Name, Title]

[Client/Authorized Signatory]