SOVERNET COMMUNICATIONS

February 3, 2016

The Commission's Secretary, Ms. Marlene H. Dortch
Office of the Secretary
Federal Commissions Communication
445 12th Street, SW, Suite TW-A325
Washington DC 20554

Annual Customer Proprietary Network Information Certification
Pursuant to 47 C.F.R. § 64.2009(e)
EB Docket No. 06-36

Name of Company:	Sovernet Fiber Corp.
Form 499 Filer ID:	828655
Name of Signatory:	Richard Kendall
Title of Signatory:	President

I, Richard Kendall, certify that I am an officer of Sovernet Fiber Corp. ("SFC"), and acting as an agent of SFC, that I have personal knowledge that SFC has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47* C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how SFC's procedures ensure the company is in compliance with the requirements set forth in sections 64.2001 *et seq.* of the Commission's rules.

SFC has not taken any actions (instituted proceedings or filed petitions at either state commissions, courts, or at the FCC) against data brokers in the past year. SFC has no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available *(e.g.,* through news media), regarding the processes pretexters are using to attempt to access CPNI. The steps the company has taken to protect CPNI include updating its CPNI practices and procedures and conducting new training designed to ensure compliance with the FCC's modified CPNI rules.

SFC has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Richard Kendall

Richard Kendall
President
Sovernet Fiber Corp.

Date: February 3, 2016

Customer Proprietary Network Information Certification – February 2016
Attachment A

SFC has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("FCC") rules pertaining to customer proprietary network information ("CPNT") set forth in sections 64.2001 — 64.201 1 of the Commission's rules. This attachment summarizes those practices and procedures, which have been updated so that they are adequate to ensure compliance with the Commission's CPNI rules, as modified by the Commission in 2007.

Safeguarding against pretexting

- SFC takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI based on customer-initiated contacts. SFC is committed to notify the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against pretexters and data brokers.

Training and discipline

- SFC trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out SFC's obligation to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, (d) obtain customers' informed consent as required with respect to its use for marketing purposes, and (e) keep records regarding customer complaints regarding CPNT and the use of CPNI for marketing campaigns.

- SFC employees are required to review SFC's CPNI practices and procedures set forth in employee personnel policies and manuals and to acknowledge their comprehension thereof with signature.

- SFC has an express disciplinary process in place for violation of the company's CPNI practices and procedures are included in employee personnel policies and manuals. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

SFC's use of CPNI

- SFC may use CPNI for the following purposes:
  - To initiate, render, maintain. repair, bill and collect for services;
  - To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
  - To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
  - To market additional services to customers that are within the same categories of service to which the customer already subscribes;
  - To market services formerly known as adjunct-to-basic services; and
  - To market additional services to customers with the receipt of informed consent via the use of opt-in or out-out, as applicable.
- SFC does not disclose or permit access to CPNI to track customers that call competing service providers.

- SFC discloses and permits access to CPNI where required by law *(e.g.,* under a lawfully issued subpoena).

Customer approval and informed consent

- SFC has implemented a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This system also allows for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.

  - Prior to any solicitation for customer approval, SFC notifies customers of their right to restrict the use of, disclosure of, and access to their CPNI.
  - SFC uses opt-in approval when using or disclosing CPNI for purposes other than permitted under opt-out approval or in 47 USC 222 and the FCC's CPNI rules.
  - A customer's approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval.
  - Records of approvals are maintained for at least one year.
  - SFC provides individual notice to customers when soliciting approval to use, disclose, or permit access to CPNI.
  - The content of SFC's CPNI notices complies with FCC rule 64.2008(c).

Opt-out and Opt-in

  - SFC does not use CPNI to market services to customers that are outside the category of services to which the customer does not already subscribe.
  - SFC does not share, disclose, or otherwise provide CPNI to third parties for marketing purposes.
  - Whenever SFC needs customer approval to use CPNI, it provides notification to its subscribers that comply with the Commission's CPNI regulations.

One-time use

- After authentication, SFC uses oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice comports with FCC rule 64.2008(f).

Additional safeguards

- SFC maintains for at least one year records of all marketing campaigns that use its customers' CPNI, including a description of each campaign and the CPNI used, the products offered as part of the campaign, and instances where CPNI was disclosed to third parties or where third parties were allowed access to CPNI. Such campaigns are subject to a supervisory approval and compliance review process, the records of which also are maintained for a minimum of one year.

- SFC has established a supervisory review process designed to ensure compliance with the FCC's CPNI rules for outbound marketing situations and maintenance of records.

- SFC designates one or more officers, as an agent or agents of the company, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in FCC rule 64.2009(e).

- SFC will provide written notice to the Commission in accordance with the requirements of FCC rule 64.2009(f) if ever its opt-out mechanisms malfunction in the manner described therein.

- SFC establishes passwords and a backup authentication method for customers to access their CPNI without utilizing readily available biographical information.

- For customer-initiated telephone inquiries regarding or requiring access to CPNI, SFC authenticates the customer (or its authorized representative), through a pre-established password, without prompting through the use of readily available biographical or account information. If the customer cannot provide a password, then SFC only discloses call detail information by sending it to the customer's address of

record, or by calling the customer at the telephone number of record.

- For online customer access to CPNI, SFC authenticates the customer (or its authorized representative) without the use of readily available biographical or account information. After the customer has been authenticated, SFC utilizes a customer-established password to authorize account access. SFC establishes passwords and has employed back-up authentication for lost or forgotten passwords consistent with the requirements of FCC rule 64.20 10(e).

- SFC discloses CPNI to customers at SFC's retail locations if the customer first presents a valid photo ID matching the customer's account information.

- SFC notifies customers immediately of any account changes, including address of record, authentication, online account and password related changes.

- SFC may negotiate alternative authentication procedures for services that SFC provides to business customers that have both a dedicated account representative and a contract that specifically addresses SFC's protection of CPNI.

- In the event of a breach of CPNI, SFC will notify law enforcement as soon as practicable and no later than seven (7) business days from discovering the breach. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs SFC to delay notification, or SFC and the investigatory party agree to an earlier notification. SFC will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved along with notifications sent to law enforcement and affected customers.

– End of Document –