Via ECSF

February 14, 2019

Marlene Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th St, SW - Room TW-A325
Washington, DC 20554

RE: Docket No. 06-36
Geneseo Telephone Company (Form 499 Filer ID 808200)

Dear Secretary Dortch:

Pursuant to §64.2009 (e) of the Commission's rule, on behalf of Geneseo Telephone Company, attached please find Geneseo Telephone Company's 2019 Annual CPNI certification and accompanying Statement of Compliance. Kindly direct any questions regarding this filing to my attention. Thank you.

Sincerely,
Scott Rubins
Vice President – Management Services

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: February 14, 2019

2. Name of company covered by this certification: Geneseo Telephone Company

3. Form 499 Filer ID: 808200

4. Name of signatory: Scott Rubins

5. Title of signatory: Vice President – Management Services

6. Certification:

I, Scott Rubins, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company 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 the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

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

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed _____

Attachments: Accompanying Statement explaining CPNI procedures

GENESEO TELEPHONY COMPANY
STATEMENT OF COMPLIANCE

Section 64.2005 Use of Customer Proprietary Network Information Without Customer Approval

The company's marketing sometimes consists of using bill inserts and direct mail – which is sent to all customers. No CPNI customer approvals are needed for this marketing. The company may also use CPNI in situations that do not require customer approval, such as marketing calling features to existing local exchange customers.

Section 64.2007 Approval Required for Use of Customer Proprietary Network Information

Section 64.2008 Notice Required for Use of Customer Proprietary Network Information

To comply with Sections 64.2007 and 64.2008 of the Commission's rules, the company requests opt-out approval in accordance with the CPNI rules. Using that consent, the company sometimes markets services to customers as allowed by the CPNI rules. For example, the company may market long distance service to local exchange customers who have not opted out. The company provides all required notices to customers on a biannual basis, and we provide such notices prior to any solicitation for customer opt-out approval. We record the customers' choices by a record indicator in the billing system. That information is readily available to the customer service representatives and marketing staff, as needed. The company does not use joint venture partners or independent contractors for marketing purposes.

Section 64.2009 Safeguards Required for Use of Customer Proprietary Network Information

The company provides periodic training sessions to our personnel to ensure they are aware of when they are and are not authorized to use CPNI. The training consists of hour-long meetings with all customer service specialists. We have an express disciplinary process in place to handle any instances where improper use is made of CPNI. This process involves written warnings and potential termination of employment for violation. For those instances where the company does use CPNI for marketing purposes, records are retained of those marketing campaigns with the details and retention periods required by the CPNI rules. We have a supervisory review process regarding compliance with the CPNI rules; we retain records of compliance as required by the rules, and sales personnel obtain supervisory approval of any proposed outbound marketing requests for opt-out approvals.

Section 64.2010 Safeguards on the Disclosure of Customer Proprietary Network Information

To ensure compliance with Section 64.2010 of the Commission's rules, telephone access to call detail information is provided only in accordance with the guidelines established in the CPNI rules. The company works with customers to establish passwords and back-up authentication methods, if requested by the customers. Telephone access to non-call detail information is only provided after the customer is authenticated. In-store access to CPNI is provided after a customer provides a valid photo ID. The company does not provide online access to CPNI without a customer provided password. The company does not have access to this password other than to reset it at the customer's directive. Whenever account information changes as specified in Section 64.2010, the company immediately notifies the customer, usually via a letter mailed to the existing address of record.

Section 64.2011 Notification of Customer Proprietary Network Information Breaches

The company trains all staff on procedures to follow to report breaches internally. We have had no breaches since this rule went into effect. When a breach is confirmed, the appropriate regulatory personnel are prepared to make the required notifications to the United States Secret Service, the Federal Bureau of Investigation, and the customer, as required and permitted under Section 64.2011. Records of such breaches and the corresponding notifications are maintained for at least two years.

Additional Measures taken by the Company to Protect Customer Proprietary Network Information

In addition to the procedures described hereinabove, other steps that the company takes to ensure the protection of Customer Proprietary Network Information include:

- Audit trails of contacts with every single customer contact
- Employee password protection to avoid unauthorized access
- Audit trails at the application and operating system levels to collect information about access by applications users and systems administrators
- Physical safeguards of the CPNI database are established to protect the database from hackers and other unauthorized attempts by third parties to access CPNI (e.g., encryption)
- Safeguards of audit trail databases
- Safeguards for the physical transfer of CPNI among companies (such as between affiliates); this could be encryption, audit trails, logs, etc.
- CPNI is not transferred to third parties, and is not disclosed to third parties for marketing purposes.
- Firewalls to prevent penetrations
- Network intrusion monitors

- Desktop web content filtering, blocking, firewalls, etc. to minimize the opportunity for infection by spyware, other malicious software and individual hacker attacks
- Physical security for sales and data centers which prevents unauthorized access to the computers which can access CPNI
- Back-up tapes are created and stored in physically secure locations
- Limits are placed on the amount of time that data is retained to limit the risk of unauthorized access