**Annual 47 CFR § 64.2009(e) CPNI Certification Template**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: 02-11-2018

2. Name of company(s) covered by this certification: NJ Telecommunication Technology, LLC

3. Form 499 Filer ID: 828323

4. Name of signatory: Niraj K. Vovra

5. Title of signatory: Consultant/Officer

6. Certification:

I, Niraj K. Vovra, 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 CFR § 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 hasn’t taken 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. [NOTE: If you reply in the affirmative, provide an explanation of any actions taken against data brokers.]

The company hasn’t received customer complaints in the past year concerning the unauthorized release of CPNI. [NOTE: If you reply in the affirmative, provide a summary of such complaints. This summary must include the number of complaints, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.]

The company represents and warrants that the above certification is consistent with 47 CFR § 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 

[*Signature of an officer, as agent of the carrier*]

# NJ TELECOMMUNICATION TECHNOLOGY, LLC.

Exhibit 1

   



ENSURE COMPLIANCE WITH



1) 

CPNI is defined in Section 222(f) of the Communications Act as

information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunication service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier customer relationship; and

information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier (except that CPNI does not include subscriber list information). Generally, CPNI includes personal information  her telecommunications services. CPNI encompasses information such as:



* + 1. The telephone numbers called by a consumer;
    2. The telephone numbers calling a customer;
    3. The time, nd and inbound

phone calls

* + 1. The telecommunications and information services purchased by a consumer.

Call Detail Records (CDR) is a category of CPNI that is particularly sensitive from a privacy standpoint and that is sought by pretexters, hackers and other unauthorized entities for illegitimate purposes. Call detail includes any information that pertains to the transmission of a specific telephone call, including the number called (for outbound calls), the number from which the call was placed (for inbound calls), and the date, time, location and/or duration of the call (for all calls).

1. Use and Disclosure of CPNI Is Restricted

The Company recognizes that CPNI includes information that is personal and individually identifiable, and that privacy concerns have led Congress and the FCC to impose restrictions upon its use and disclosure, and upon the provision of access to it by individuals or entities inside and outside the Company. The Company has designated a CPNI Compliance Officer who is responsible for:

Communi   responsibilities, requirements and restrictions;



Supervising the training of Company employees and agents who use or have access to CPNI;

Supervising the use, disclosure, distribution   independent contractors and joint venture partners;

Maintaining records regarding the use of CPNI in marketing campaigns;

Receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI.

Company employees and agents that may deal with CPNI have been informed that there are substantial federal restrictions upon CPNI use, distribution and access. In order to be authorized

  oyees and agents must receive training with respect to the requirements of Section 222 of the Communications Act and the



(Subpart U of Part 64 of the FCC Rules).

Before an agent, independent contractor or joint venture partner may receive or be allowed to



 agent, independent contractor or joint venture partner must enter into an additional confidentiality agreement which provides) that:

1. The agent, independent contractor or joint venture partner may use the CPNI only for the purpose for which the CPNI has been provided;
2. The agent, independent contractor or joint venture partner may not disclose or distribute the CPNI to, or allow access to the CPNI by, any other party (unless the agent, independent contractor or joint venture partner is expressly and specifically required to do so by a court order);
3. The agent, independent contractor or joint venture partner must implement appropriate and specific safeguards acceptable to the Company to ensure the confidentiality of the
4. Protection of CPNI

The Company may, after receiving an appropriate written request from a customer

address or record. Any and all such customer requests:

* 1. must be made in writing;
  2. must  d

telephone number;

* 1. must specify exactly what type of CPNI must be disclosed or provided;
  2. must specify the time period for which the CPNI must be disclosed or provided; and
  3. must be signed by the customer. The Company will disclose CPNI upon affirmative written request by the customer to any person designated by the customer, but only after the Company calls the



of

record to verify the accuracy of this request.

             

enforcement agency in accordance with applicable legal requirements.

Since inception  

question-answer combinations in secure files that may be accessed only by authorized Company employees who need such information in order to

authenticate the identity of customers requesting call detail information over the telephone.

Since inception Company employees authenticate all telephone requests for CPNI in the same manner whether or not the CPNI consists of call detail information. That is, Company employees must:

1. -established password (or correct answers to the back-



1. send the requested 



(see definition above) with the requested information.



If a customer subscribes to multiple services offered by the Company and an affiliate, the    services with its affiliate. If a customer does not subscribe to any telecommunications or non-telecommunications services offered by an affiliate,

with the affiliate



approval



procedures set forth in Se Rules.



When an existing customer calls the Company to inquire about or order new, additional or modified services (in-bound marketing), the Company may use the

than call detail CPNI to assist the customer for the Company provides the customer with the



oral notice required by Sections 64.2008(c) and 



and after the Company authenticates the customer. Since inception, the Company discloses or releases call detail information to customers during customer-initiated telephone contacts only when the customer provides a pre-established password. If the customer does not provide a password, call detail information is released only   carrier calling the



customer at the telephone number of record. If the customer is able to provide to the Company during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and, if applicable, the amount charged for the call) without Company assistance, then the Company may take routine customer service actions related to such information. (However, under this circumstance, the Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.)

The Company uses, discloses, and/or permits access to CPNI in connection with Company-initiated marketing of services to which a customer does not already subscribe from the Company (out-bound marketing) only pursuant to the notice and approval procedures set forth in Sections 64.2007, 64.2008, and 64.2009 of proposed out-bound marketing activities are reviewed by the



  Officer for compliance with the CPNI restrictions and requirements in the Communications Act and the FCC Rules.

The Company maintains appropriate paper and/or electronic records that allow its employees, independent contractors and joint venture partners to clearly establish the status -out and/or Opt-In approvals (if any) prior to use CPNI. These records include: (i) the date(s) of any and all of the



-out approvals and/or Opt-in approvals, together with the dates of any modifications or revocations of such approvals; and (ii) the type(s) of CPNI use, access, disclosure and/or distribution approved by the customer.

-bound marketing activity or

campaign,



NI approval. Company employees, independent contractors and

joint venture partners are required to notify the CPNI Compliance Officer of any access, accuracy or security problems they encounter with respect to these records. If new, additional or extended approvals are necessary, the CPNI Compliance Officer will  -Out CPNI

- used with respect to various proposed out-bound marketing activities.

The CPNI Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including:

* 1. a description of the campaign;
  2. the specific CPNI that was used in the campaign;
  3. the date and purpose of the campaign:
  4. What products and services were offered as part of the campaign? This record shall be maintained for a minimum of one year.

bill and collect for telecommunications services. The Company may obtain information from new or existing customers that may constitute CPNI as part of applications or requests for new, additional or modified services, and its employees and agents may use such customer information (without further customer approval) to initiate and provide the services. Likewise, the Comp employees and billing agents may use customer service and calling records (without customer approval):

1. To bill customers for services rendered to them;



1. To investigate and resolve disputes with customers regarding their bills;
2. To pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.
3. 



approval to  

and other carriers from fraudulent, abusive or illegal use of (or subscription to) the telecommunications service from which the CPNI is derived. Because allegations and investigations of fraud, abuse and illegal use constitute very sensitive matters, any access, use, disclosure or distribution of CPNI pursuant to this Section must be expressly approved

  Officer.



partners may NOT use CPNI to identify or track customers who have made calls

to, or received calls   

employees, agents, independent contractors or joint venture partners use or disclose CPNI for personal reasons or profit.

Company policy mandates that files containing CPNI be maintained in a secure manner such that they cannot be used, accessed, disclosed or distributed by unauthorized individuals or in an unauthorized manner.

Paper files containing CPNI are kept in secure areas, and may not be used, removed, or copied in an unauthorized manner.

Electronic files and databases containing CPNI are maintained on computers that are not 



firewalls that are regularly monitored and tested for effectiveness. In addition, such electronic files and databases may be accessed only by authorized Company employees who have been provided a currently effective strong login ID and password which will be changed periodically).

Company employees, agents, independent contractors and joint venture partners are required to notify the CPNI Compliance Officer of any access or security problems they encounter with respect to files containing CPNI.

The Company may permit its customers to establish online accounts, but must require an appropriate password to be furnished by the customer before he or she can access any CPNI in his or her online account. Since December 8, 2007, passwords may NOT be based upon readily obtainable biographical information (e.g., the name, social security number or date of birth) or account information (e.g. telephone number or address).



Since its inception the company provides the customers an initial or replacement password:

* 1. If they   

  other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address;



* 1. If they call a specified Company telephone number from their telephone number of record, and then wait at that number until a Company representative calls them back and obtains correct answers to certain questions regarding their service and address.

Since inception the Company notifies the customers immediately of certain changes in their accounts that may affect privacy or security matters.

1. The types of changes that require immediate notification include: (a) change or request   r



request for change of the n record; (c) change or request for change of any significant element

account; and (d) a change or request for change to the

responses with respect to the back-up means of authentication for lost or forgotten passwords.

1. The notice may be provided by: (a) a Company call or voicemail to the telephone number of record; (b) a Company text message to number of record; or (c) a written notice mailed



  address on

record).

1. The notice must identify only the general type of change and must not reveal the changed information.
2. The Company employee or agent sending the notice must prepare and furnish to the CPNI Compliance Officer a memorandum containing:
   1. the name, address of record, and telephone number of record of the customer notified;
   2. a copy or the exact wording of the text message, written notice, telephone message or voicemail message comprising the notice;
   3. the date and time that the notice was sent.

Since inception the Company has been providing notices to the customer if a security breach results in the disclosure of the 



i. As soon as practicable (and in no event more than seven (7) days) after the Company discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used or disclosed CPNI, the Company must provide electronic notification of such breach to the United States Secret Service and to the Federal Bureau of Investigation via a central reporting facility accessed through a link maintained by the FCC at [http://www.fcc.gov/eb/cpni.](http://www.fcc.gov/eb/cpni)

The Company and its authorized employees may use CPNI to provide call location information regarding mobile users in certain emergency situations. Except in an unforeseen emergency involving a substantial threat to human life or safety, any and all use or provision of CPNI under this category must involve the specific types or categories of emergencies listed in wr   CPNI Compliance Officer.

Since December 8, 2007, the Company will provide customers with access to CPNI at its retail locations if the customer presents a valid photo ID and the valid photo ID matches the name on the account.

Since December 8, 2007, the Company takes reasonable measures to discover and protect against activity that is indicative of pretexting including requiring Company employees, agents, independent contractors and joint venture partners to notify the CPNI Compliance Officer immediately by voice, voicemail or email of:

1. any suspicious or unusual call 

information or other CPNI (including a call where the caller furnishes an incorrect password or incorrect answer to one or both of the

-answer combinations);

1. any suspicious or unusual attempt by an 

password or account information (including providing inadequate or



1. any and all discovered

files or databases containing passwords or CPNI was denied due to the provision of incorrect logins and/or passwords; and

1. any complaint by a customer of unauthorized or inappropriate use or disclosure of his or her CPNI. The CPNI Compliance Officer will request further information in writing, and investigate or supervise the investigation of, any incident or group of incidents that reasonably appear to entail pretexting.
2. CPNI Compliance Officer

In addition to the specific matters required to be reviewed and approved by the

contractors and joint venture partners are strongly encouraged to bring any and all other questions, issues or uncertainties regarding the use, disclosure, or access to

         



investigation, review and guidance. The extent to which a particular employee or agent brought a CPNI matter to the attention of the CPNI Compliance Officer and received appropriate guidance is a material consideration in any disciplinary action brought against the employee or agent for impermissible use, disclosure or access to CPNI.

1. Disciplinary Procedures

The Company has informed its employees and agents, independent contractors and joint venture partners that it considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be very important. Violation by Company employees or agents of such CPNI requirements will lead to disciplinary action (including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from the CPNI Compliance Officer, and the extent to which the violation was or was not deliberate or malicious). Violation by Company independent contractors or joint venture partners of such CPNI requirements will lead to prompt disciplinary action (up to and including remedial training and termination of the contract)

1. Safeguard of customers and callsdata

All the Servers owned by NJ TELECOMMUNICATION TECHNOLOGY LLC is hosted in a secure data center and encrypted with best technology and armed with firewall and antivirus software, the databases are very secure and are encrypted with the latest technology, and servers are checked regularly for any unusual activity, so far the company has not stored any critical information related to the customer CPNI in a insecure system, the Operating System is upgraded and checked regularly by professionals. The company cares about the privacy and protects the customers data with care. The old call records are archived and backed up in an encrypted drive.