NORTH DAKOTA NETWORK COMPANY

A SUBSIDIARY OF SRT COMMUNICATIONS, INC

PO Box 2027 • Minot, ND 58702
701-858-1200 • 1-800-737-9130

January 15, 2018

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

RE: CPNI COMPLIANCE CERTIFICATE [SECTION 64.2009(e) of FCC RULES]
EB DOCKET NO. 06-36

Following is the Annual 64.2009(e) CPNI Certification for the year 2017 for North Dakota Network Co. ("NDNC"), dba SRT Wireless.

SRT Communications, Inc., FCC Form 499 Filer ID 816412

Also attached is the "Statement Explaining How NDNC's Operating Procedures Ensure Compliance with the FCC's CPNI Rules", the "Statement of Action Taken Against Data Brokers", and "Summary of Customer Complaints Regarding Unauthorized Release of CPNI".

Sincerely,

John A. Reiser
COO

CPNI COMPLIANCE CERTIFICATE
[Section 64.2009(e) of FCC Rules]

EB DOCKET NO. 06-36

I hereby certify that I am an Officer of NDNC, dba SRT Wireless, and am executing this CPNI Compliance Certificate as its agent.

I have personal knowledge that NDNC has established operating procedures that are adequate to ensure compliance with the Customer Proprietary Network Information rules and requirements in Subpart U of Part 64 of the Federal Communications Commission's Rules (47 C.F.R. §§64.2001 through 64.2011).

The "Statement Explaining How NDNC's Operating Procedures Ensure Compliance With the FCC's CPNI Rules" attached explains how NDNC's operating procedures ensure that it is in compliance with the foregoing FCC rules during the subject Calendar Year.

The "Statement of Actions Taken Against Data Brokers" attached describes any actions taken by SRT against data brokers during the subject Calendar Year.

The "Summary of Customer Complaints Regarding Unauthorized Release of CPNI" attached lists the numbers of various types of customer complaints received by SRT during the subject Calendar Year concerning the unauthorized use of CPNI.

I am making this certification for Calendar Year 2017.
FCC Filer ID: 816412

Signature

John A. Reiser, Chief Operating Officer
Printed Name and Title

1-15-18

Date

STATEMENT EXPLAINING HOW SRT'S OPERATING PROCEDURES ENSURE COMPLIANCE WITH THE FCC'S CPNI RULES

NORTH DAKOTA NETWORK CO.
"SRT WIRELESS"

I. Customer Proprietary Network Information ("CPNI")

CPNI is defined in Section 222(f) of the Communications Act as (A) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications 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 (B) 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 regarding a consumer's use of his or her telecommunications services. CPNI encompasses information such as: (a) the telephone numbers called by a consumer; (b) the telephone numbers calling a customer; (c) the time, location and duration of a consumer's outbound and inbound phone calls, and (d) the telecommunications and information services purchased by a consumer.

Call detail information (also known as "call records") 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).

II. Use and Disclosure of CPNI Is Restricted

SRT 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 SRT.

SRT has designated a CPNI Compliance Officer who is responsible for: (1) communicating with SRT's attorneys and/or consultants regarding CPNI responsibilities, requirements and restrictions; (2) supervising the training of SRT employees and agents who use or have access to CPNI; (3) supervising the use, disclosure, distribution or access to SRT's CPNI by independent contractors and joint venture partners; (4) maintaining records regarding the use of CPNI in marketing campaigns; and (5) receiving, reviewing and resolving questions or issues regarding use, disclosure, distribution or provision of access to CPNI. SRT 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 to use or access SRT's CPNI, employees and agents must receive training with respect to the requirements of Section 222 of the Communications Act and the FCC's CPNI Rules (Subpart U of Part 64 of the FCC Rules).

Before an agent, independent contractor or joint venture partner may receive or be allowed to access or use SRT's CPNI, the agent's, independent contractor's or joint venture partner's agreement with SRT must contain provisions (or SRT and the agent, independent contractor or joint venture partner must enter into an additional confidentiality agreement which provides) that: (a) the agent, independent contractor or joint venture partner may use the CPNI only for the purpose for which the CPNI has been provided; (b) 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); and (c) the agent, independent contractor or joint venture partner must implement appropriate and specific safeguards acceptable to SRT to ensure the confidentiality of SRT's CPNI.

III. Protection of CPNI

1. SRT may, after receiving an appropriate written request from a customer, disclose or provide the customer's CPNI to the customer by sending it to the customer's address or record. Any and all such customer requests: (1) must be made in writing; (2) must include the customer's correct billing name and address and telephone number; (3) must specify exactly what type or types of CPNI must be disclosed or provided; (4) must specify the time period for which the CPNI must be disclosed or provided; and (5) must be signed by the customer. SRT will disclose CPNI upon affirmative written request by the customer to any person designated by the customer, but only after SRT calls the customer's telephone number of record and/or sends a notification to the customer's address of record to verify the accuracy of this request.

2. SRT will provide a customer's phone records or other CPNI to a law enforcement agency in accordance with applicable legal requirements.

3. Since December 8, 2007, SRT will retain all customer passwords and "shared secret" question-answer combinations in secure files that may be accessed only by authorized SRT employees who need such information in order to authenticate the identity of customers requesting call detail information over the telephone.

4. Since December 8, 2007, SRT employees will ask for a password, or "shared secret" answers, for telephone requests inquiring about call detail information. That is, SRT employees must: (a) be furnished with the customer's pre-established password (or correct answers to the back-up "shared secret" combinations);

(b) send the requested information to the customer's postal or electronic "address of record" (see definition above);" or (c) call the customer back at the customer's "telephone number of record" (see definition above) with the requested information.

If the customer has the specific call detail information readily available, the SRT employee will proceed with the call.

5. SRT has adopted a policy that it does not and will not use, disclose or permit access to CPNI by an affiliate.

6. When an existing customer calls SRT to inquire about or order new, additional or modified services (in-bound marketing), SRT may use the customer's CPNI other than call detail CPNI to assist the customer for the duration of the customer's call if SRT provides the customer with the oral notice required by Sections 64.2008(c) and 64.2008(f) of the FCC's Rules and after SRT authenticates the customer.

Since December 8, 2007, SRT may disclose or release 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 can be released only by sending it to the customer's address of record or by the carrier calling the customer at the telephone number of record. If the customer is able to provide to SRT 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 SRT assistance, then SRT may take routine customer service actions related to such information. (However, under this circumstance, SRT 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.)

7. SRT has adopted a policy that it does not and will not use, disclose, or permit access to CPNI in connection with SRT-initiated marketing of services to which a customer does not already subscribe from SRT (out-bound marketing).

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

9. Before a customer's CPNI can be used in an out-bound marketing activity or campaign, SRT's records must be checked to determine the status of the customer's CPNI approval. SRT 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.

10. The CPNI Compliance Officer will maintain a record of each out-bound marketing activity or campaign, including: (i) a description of the campaign; (ii) the specific CPNI that was used in the campaign; (iii) the date and purpose of the campaign: and (iv) what products and services were offered as part of the campaign. This record shall be maintained for a minimum of one year.

11. SRT's employees and billing agents may use CPNI to initiate, render, bill and collect for telecommunications services. SRT 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, SRT's employees and billing agents may use customer service and calling records (without customer approval): (a) to bill customers for services rendered to them; (b) to investigate and resolve disputes with customers regarding their bills; and (c) to pursue legal, arbitration, or other processes to collect late or unpaid bills from customers.

12. SRT's employees and agents may use CPNI without customer approval to protect SRT's rights or property, and to protect users 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 in advance and in writing by SRT's CPNI Compliance Officer.

13. SRT's employees, agents, independent contractors and joint venture partners may **NOT** use CPNI to identify or track customers who have made calls to, or received calls from, competing carriers. Nor may SRT's employees, agents, independent contractors or joint venture partners use or disclose CPNI for personal reasons or profit.

14. SRT 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.

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

16. Electronic files and databases containing CPNI are maintained on computers that are not accessible from the Internet or that are on SRT's intranet behind firewalls that are regularly monitored and tested for effectiveness. In addition, such electronic files and databases may be accessed only by authorized SRT employees who have been provided a currently effective strong login ID and password (which password is periodically changed).

17. SRT 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.

18. SRT 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. Such password may NOT be based upon readily obtainable biographical information (*e.g.*, the customer's name, mother's maiden name, social security number or date of birth) or account information (*e.g.*, the customer's telephone number or address).

19. Since December 8, 2007, Customers may obtain an initial or replacement password: (i) if they come in person to SRT's business office, produce a driver's license, passport or other government-issued identification verifying their identity, and correctly answer certain questions regarding their service and address; or (ii) if they call a specified SRT telephone number from their telephone number of record, and then wait at that number until a SRT representative calls them back and obtains correct answers to certain questions regarding their service and address.

20. Since December 8, 2007, SRT will notify customers immediately of certain changes in their accounts that may affect privacy or security matters.

a. The types of changes that require immediate notification include: (a) change or request for change of the customer's password; (b) change or request for change of the customer's address of record; (c) change or request for change of any significant element of the customer's online account; and (d) a change or request for change to the customer's responses with respect to the back-up means of authentication for lost or forgotten passwords.

b. The notice may be provided by: (a) a SRT call or voicemail to the customer's telephone number of record; (b) a SRT text message to the customer's telephone number of record; or (c) a written notice mailed to the customer's address of record (to the customer's prior address of record if the change includes a change in the customer's address of record).

c. The notice must identify only the general type of change and must not reveal the changed information.

d. SRT employee or agent sending the notice must prepare and furnish to the CPNI Compliance Officer a memorandum containing: (a) the name, address of record, and telephone number of record of the customer notified; (b) a copy or the exact wording of the text message, written notice, telephone message or voicemail message comprising the notice; and (c) the date and time that the notice was sent.

21. Since December 8, 2007, SRT must provide an initial notice to law enforcement and a subsequent notice to the customer if a security breach results in the disclosure of the customer's CPNI to a third party without the customer's authorization.

a. As soon as practicable (and in no event more than seven (7) days) after SRT discovers that a person (without authorization or exceeding authorization) has intentionally gained access to, used or disclosed CPNI, SRT 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.

22. SRT 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 writing by SRT's CPNI Compliance Officer.

23. Since December 8, 2007, SRT 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.

24. Since December 8, 2007, SRT takes reasonable measures to discover and protect against activity that is indicative of pretexting including requiring SRT employees, agents, independent contractors and joint venture partners to notify the CPNI Compliance Officer immediately by voice, voicemail or email of: (a) any suspicious or unusual call requesting a customer's call detail information or other CPNI (including a call where the caller furnishes an incorrect password or incorrect answer to one or both of the "shared secret" question-answer combinations); (b) any suspicious or unusual attempt by an individual to change a customer's password or account information (including providing inadequate or inappropriate identification or incorrect "address or record," "telephone number of record" or other significant service information); (c) any and all discovered instances where access to SRT's electronic files or databases containing passwords or CPNI was denied due to the provision of incorrect logins and/or passwords; and (d) 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.

IV. CPNI Compliance Officer

In addition to the specific matters required to be reviewed and approved by SRT's CPNI Compliance Officer, employees and agents, independent 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 CPNI to the attention of SRT's CPNI Compliance Officer for appropriate 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.

V. Disciplinary Procedures

SRT 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 SRT 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 SRT 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).

SRT'S STATEMENT OF ACTION TAKEN AGAINST DATA BROKERS
NORTH DAKOTA NETWORK CO.
"SRT WIRELESS"

A. During Calendar Year **2017**, SRT has instituted the following proceeding, or filed the following petitions, against data brokers before the Federal Communications Commission:

NONE

B. During Calendar Year **2017**, SRT has instituted the following proceeding, or filed the following petitions, against data brokers before the North Dakota Public Service Commission:

NONE

C. During Calendar Year **2017**, SRT has instituted the following proceeding, or filed the following petitions, against data brokers:

NONE

D. During Calendar Year **2017**, SRT did not take any actions against data brokers because, to the best of SRT's knowledge, no data broker attempted to obtain any call detail information or other CPNI from SRT during the year.

SRT'S SUMMARY OF CUSTOMER COMPLAINTS REGARDING UNAUTHROIZED RELEASE OF CPNI
NORTH DAKOTA NETWORK CO.
"SRT WIRELESS"

A. During Calendar Year **2017**, SRT has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access by SRT employees:

NONE

B. During Calendar Year **2017**, SRT has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper disclosure to individuals not authorized to receive the information:

NONE

C. During Calendar Year **2017**, SRT has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access to online information by individuals not authorized to view the information:

NONE

D. During Calendar Year **2017**, SRT has become aware of the following processes that pretexters are using to attempt to access its CPNI:

NONE