Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

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

1. Date filed: February 20, 2018

2. Name of companies covered by this certification and 499 Filer IDs:

Northland Communications Corporation	
Northland Cable Properties, Inc.	826515
Northland Cable Television, Inc.	826497
Northland Cable Ventures LLC	826517

3. Name of signatory: Paul Milan
4. Title of signatory: Vice President and General Counsel

5. Certification:

I, Paul Milan, certify that I am an officer of Northland Communications Corporation, which is the manager of Northland Cable Properties, Inc.; Northland Cable Television, Inc.; and Northland Cable Ventures LLC (together, the "Company"), and, acting as an agent of each of these companies, that I have personal knowledge that the Company has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Federal Communications Commission's customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how Company's procedures ensure that the Company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq*. of the Commission's rules.

The Company has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. Company has not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject the Company to enforcement actions.

Paul Milan
Vice President and General Counsel
Northland Communications Corporation
Executed February 6, 2018

NORTHLAND COMMUNICATIONS CORPORATION
CONSUMER PROPRIETARY NETWORK INFORMATION POLICY

Revised Effective March 1, 2016

This document, the Northland Communications Corporation Consumer Proprietary Network Information Policy (the "Policy"), sets forth Northland Communications Corporation and its affiliates' (collectively, "Northland") policies and procedures regarding the confidentiality of Customer Proprietary Network Information ("CPNI") and to ensure compliance with the CPNI rules of the Federal Communications Commission ("FCC"). CPNI is defined as follows:

> (A) information that relates to the quantity, technical configuration, type, destination, location, 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.

The Policy is designed to protect the confidentiality of CPNI and ensure compliance with the FCC's rules set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*. To ensure compliance with the FCC's rules, Northland trains employees on the limitations of use or disclosure of CPNI as governed by Federal law and the Policy. The Policy is administered by its CPNI Compliance Officer, Paul Milan, General Counsel.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Northland will use, disclose or permit access to individually identifiable CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Northland, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer. Northland does not use CPNI to market service offerings among the different categories of service, or even within the same category of service that it provides to subscribers. If Northland changes the Policy, Northland shall conduct additional training as needed to assure compliance with the FCC's rules. Northland does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Northland takes reasonable measures to protect against attempts to gain unauthorized access to CPNI. Employees with access to CPNI, including Customer Service Representatives ("CSRs"), are trained in procedures emphasizing, among other points, that they be cognizant that unauthorized persons may have significant apparent familiarity with a customer's biographical and account information. If any CSR becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Northland's existing policies that would strengthen protection of CPNI, the CSR is instructed to report such information immediately to their supervisor (who in turn will refer the report to the CPNI Compliance Officer as appropriate) so that Northland may evaluate whether existing policies should be supplemented or changed.

A. Online Access to CPNI

CPNI is made available online to Northland's customers through Northland's third-party vendors' online service websites. The websites may contain service information, including billing information, and phone, Internet, video and/or ancillary services billing information, and have tools that allow the customer to customize their calling features. To access CPNI online, a customer must first register in the online system. To register, the customer must create a unique password. The password is not accessible by Northland. Once registered, a customer may access their account using their email and password. If a customer forgets their password, they can request that their password be reset and an email is sent to the address they entered into the system at registration. If a customer changes their password, email address or mailing address, a confirmation email is sent to their email address (and in the case of a change in email, to their prior email address) as confirmation.

B. Inbound Calls to Northland Requesting CPNI

Call Detail Information (CDI) is a subset of CPNI that includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. Northland does not provide CDI to inbound callers. Northland may send a copy of a bill or requested CDI to the mailing address of record for the account, but only if such address has been on file with Northland for at least thirty (30) days. If Northland has reason to believe that an inbound caller seeking CDI may not be an authorized person, Northland notes the account. If a third event is noted, Northland restricts

disclosure of all CDI over the telephone until Northland is able to verify whether such inquiries were made by an authorized person.

For CPNI other than CDI, CSRs are trained to require an inbound caller to authenticate their identity using methods appropriate for the information sought prior to revealing any CPNI or account information to the caller.

C. In-Person Disclosure of CPNI at Northland's Offices

Northland may disclose CPNI to an authorized person at a Northland office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

D. Notice of Account Changes

When an account is created or the address of record is changed, except in connection with the customer's initiation of service, Northland sends a notice to customer's pre-existing email or mailing address of record notifying them of the change. When an online account password is created or changed, or a customer address of record is changed via the online portal, a notice is sent to the customer's email address of record notifying them of the change. Such notice will not reveal the changed information and will direct the customer to notify Northland immediately if they did not authorize the change.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Northland acknowledges that Federal law imposes specific requirements upon Northland in the event that Northland becomes aware of any breach of customer CPNI. A breach includes any instance in which any person has intentionally gained access to, used or disclosed a Northland customer's CPNI beyond their authorization to do so. Any Northland employee who becomes aware of any breaches (as defined below), suspected breaches or attempted breaches must report such information immediately to Northland's CPNI Compliance Officer, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee who fails to report such information will be subject to disciplinary action that may include termination.

It is Northland's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law

enforcement promptly. Therefore, although employees who violate Northland's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations, if appropriate.

Northland's CPNI Compliance Officer is currently Paul Milan, General Counsel, who may be contacted at (206) 621-1351.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used or disclosed CPNI. If an employee has information about an incident and is not certain if the incident would constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer.

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, Northland's CPNI Compliance Officer shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. If this link is not responsive, Northland will contact the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/eb/cpni) for instructions. Northland will not notify customers or disclose a breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI except as provided below (a full business day does not count a business day on which the notice was provided). Federal law requires compliance with this requirement even if state law requires disclosure. If Northland receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach. Northland is not required to inform customers whose CPNI was not actually disclosed.

Northland will delay notification to customers or the public upon request of the FBI or USSS. If Northland's CPNI Compliance Officer believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Northland may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

IV. RECORD RETENTION

Northland CPNI Compliance Officer is responsible for maintaining a record, electronically or in some other manner, covering any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers over the prior

two-year period. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach and the circumstances of the breach.

Northland maintains a record, for a period of at least one (1) year, of (i) circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI, and (ii) supervisory review of marketing that proposes to use CPNI or to request customer approval to disclose CPNI.

Northland maintains a record of all customer complaints related to Northland's handling of CPNI, and records of Northland's handling of such complaints, for at least two (2) years. The CPNI Compliance Officer will assure that all complaints are reviewed and that Northland considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

An authorized corporate officer, as an agent of Northland, will sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Northland has established operating procedures that are adequate to ensure compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Northland's operating procedures ensure compliance with the FCC's CPNI rules. In addition, the filing will include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

All employees with access to CPNI receive a copy of Northland's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Northland requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel. The CSR training emphasizes, among other points, that employees be cognizant that some unauthorized persons may have significant apparent familiarity with a customer's biographical and account information.