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 23, 2018
2. Name of company covered by this certification: Cablevision of Marion County, LLC d/b/a Fibervision
3. Form 499 Filer ID: 826274
4. Name of signatory: Kerri King
5. Title of signatory: President
6. Certification:

I, Kerri King, certify that I am an officer of Cablevision of Marion County, LLC d/b/a Fibervision ("Company") and, acting as an agent of the Company, 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 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*.

The Company has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. The Company has not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either the Florida Public Service Commission, 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 a filer to enforcement actions.

Kerri King
President
Cablevision of Marion County, LLC
Executed February 23, 2018

CPNI Compliance Policies of
Cablevision of Marion County, LLC d/b/a Fibervision

The following summary describes the policies of Cablevision of Marion County, LLC d/b/a Fibervision ("Company") that are designed to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*

CPNI is "(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 Company's policy, administered by its CPNI Compliance Officer, Kerri King, establishes the following parameters regarding the use and disclosure of CPNI:

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Company will use, disclose, or permit access to 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 the Company, 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. Company 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. Although current Company policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve a supervisor designated by a senior employee responsible for marketing and the CPNI Compliance Officer. If such use is approved, Company shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When Company receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, Company will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee 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 Company's existing policies that would strengthen protection of CPNI, they should report such information immediately to Company's CPNI Compliance Officer so that Company may evaluate whether existing policies should be supplemented or changed.

A. Assignment of Personal Identification Numbers

Company now assigns a randomly-generated Personal Identification Number (PIN) for each new telephone account. Because the PIN is randomly assigned, it is not expected to consist of any material portion of the customer's account number, telephone number, street address, zip code, social security number, date of birth, or other biographical or account information. PINs will also not consist of easily-guessed numbers.

Customers who do not have PINs, who have forgotten their PIN, or who wish to change their PIN may request that a new PIN be created for their account. The new PIN will be provided to the customer by mailing it to their address of record, or by providing to them through an outbound call to their telephone number of record. Company may also change a PIN if it has reason to believe that the security of the PIN has been compromised.

B. Inbound Calls to Company Requesting CPNI

Call Detail Information (CDI) 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. Company will not provide CDI to an inbound caller except under the following conditions:

- A CSR can reveal CDI if the caller provides the PIN associated with their account.
- The CSR may offer to call the caller back at the customer's telephone number of record. The CSR may not rely on Caller ID information to assume that the caller is calling from such number; they must disconnect the inbound call and make a new outbound call to that number.
- Company may send a copy of a bill or requested CDI to an address of record for the account, but only if such address has been on file with Company for at least 30 days.

If an inbound caller is able to provide to the CSR the telephone number called, when it was called, and, if applicable, the amount charged for the call, exactly as that information appears in the Company's records, then the CSR is permitted to discuss customer service pertaining to that call and that call only. If the detail provided by the caller does not match on all categories, the

CSR is trained to not inform the caller which portion of the detail does not match (for example, they should not tell the customer there were no calls during a particular hour or that there are no calls to a particular number). CSRs are trained to understand that a pretexter may be as interested to know about the absence of a particular call as its existence.

For CPNI other than CDI, CSRs require an inbound caller to authenticate their identity through the telephone number, account number, and/or the name and address of record, prior to revealing any CPNI or account information to the caller.

C. Online Accounts

To access Company's online portal that provides access to CPNI, the customer must enter a password established in accordance with the criteria set forth below.

When a Customer establishes service, they are asked to choose a password for their online account. If a password is not established at that time, then they are instructed by the Company installation personnel to establish a password during the portion of the installation process at which the installer assists them with their initial log-in to the portal. When establishing or changing a password, the customer is instructed that passwords should not consist of any portion of their account number, telephone number, street address, social security number, date of birth, words, or easily-guessed strings of characters.

After the customer logs in to the portal for the first time, they are instructed to enter an email address of record for their account. This email address can only be changed online after the user has correctly entered their password.

If a customer forgets the password they have established for online access, they are given the option to request that a new, randomly-assigned password be emailed to their email address of record. If they cannot access that email account, they must call Company and ask to have a new password provided to them over the phone, if they can provide their PIN, or mailed to their address of record that has been on file with Company for at least 30 days. Because the new passwords created by Company are randomly assigned, they are not expected to consist of any material portion of the customer's account number, telephone number, street address, social security number, date of birth, words, or easily-guessed strings of characters.

D. In-Person Disclosure of CPNI at Company Offices

Company may disclose a customer's CPNI to an authorized person visiting a Company 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.

E. Notice of Account Changes

Company will send a notification to a customer's address of record immediately whenever a password, online account, or address of record is created or changed, except for such events that occur during the period when the customer initiates service, including the initial installation visit. When such a change is made to an address of record, the notice will be sent only to a prior

address of record. The notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Company immediately if they did not authorize the change.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Company employee that becomes aware of any breaches, suspected breaches or attempted breaches of CPNI must report such information immediately to the Company 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 that fails to report such information will be subject to disciplinary action that may include termination.

It is Company'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 our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate the Company's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

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 that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer.

If a Company employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Company's CPNI Compliance Officer who will determine whether to report the incident to law enforcement. Company's Compliance Officer will determine whether it is appropriate to update Company's CPNI policies or training materials in light of the new information; the FCC's rules require Company on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the Company 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. Company's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/eb/cpni) for instructions.

Company will not under any circumstances notify customers or disclose a breach to the public until 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 Company 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.

Company will delay notification to customers or the public upon request of the FBI or USSS. If the Company 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; Company still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

IV. RECORD RETENTION

The Company CPNI Compliance Officer is responsible for assuring that the Company maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. 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.

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

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

Company will have an authorized corporate officer, as an agent of the Company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Company has established operating procedures that are adequate to ensure its 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 Company's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must 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.

V. TRAINING

Company employees must use a unique login and password to obtain access to databases that include CPNI. All employees with such access receive a copy of Company'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, Company requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.