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

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

1. Date filed: February 20, 2018
2. Company covered by this certification: RM Greene, Inc. d/b/a Cable TV of East Alabama
3. Form 499 Filer ID: 825573
4. Name of signatory: Lynne G. Frakes
5. Title of signatory: President
6. Certification:

I, Lynne G. Frakes, certify that I am President and thereby an officer of RM Greene, Inc. d/b/a Cable TV of East Alabama ("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 Commission's rules, 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, 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. The Company has not taken any actions in the past calendar 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.

Lynne G. Frakes
Lynne G. Frakes
President
RM Greene, Inc.
Executed February 15, 2018

CPNI COMPLIANCE POLICIES OF CABLE TV OF EAST ALABAMA

The following summary describes the policies of Cable TV of East Alabama ("CTVEA") 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."

CTVEA's policies regarding the use and disclosure of CPNI are administered by CTVEA's CPNI Compliance Manager Lynne G. Frakes.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

CTVEA 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 CTVEA, or to protect users or other carriers or service providers from fraudulent or illegal 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.

CTVEA does not 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 the senior employee responsible for marketing and the CPNI Compliance Manager. If such use is approved, CTVEA shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

CTVEA 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

Above and beyond the specific FCC requirements, CTVEA 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 CTVEA's existing policies that would strengthen protection of CPNI, they should report such information immediately to CTVEA's CPNI Compliance Manager so that CTVEA may evaluate whether existing policies should be supplemented or changed.

A. Assignment of Personal Identification Numbers

At the time of service installation, CTVEA provides the customer a randomly-generated six-digit Personal Identification Number (PIN) for each 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 such as 000000 or 123456.

CTVEA will change a PIN upon the request of a customer (if customer provides current PIN or presents a photo ID at a company business office) or if it has reason to believe that the security of the PIN has been compromised.

B. Inbound Calls to CTVEA 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. CTVEA 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.
- If an inbound caller does not know the PIN for the account but 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 on the bill, then the CSR is permitted to discuss customer service pertaining to that call and that call only.
- The CSR may encourage the caller to obtain CDI from the password-protected on-line portal described in Section II.C. below.
- 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.
- The CSR may offer to send a copy of a bill or requested CDI to a mailing address of record for the account, but only if such address has been on file with CTVEA for at least 30 days.

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

C. Online Accounts

To access an on-line account from which a customer can access their CPNI, customer must enter a unique login ID that they create and a password established in accordance with the terms set forth below.

The first instance in which a customer seeks to obtain access, they are required to enter their account number and PIN. After correct entry of this information, the user must enter an email address of record for their account and a password for their online account.

The email address of record and password can only be changed in the future only online and only after the user has correctly entered their login ID and password, except for the process for resetting a password described below.

In the event that a customer later forgets their Login ID or password, they may enter a request on the web portal that causes the information to be sent to the email address of record. They may also submit a request to reset their password; to reset a password, the user must enter their account number and PIN.

D. In-Person Disclosure of CPNI at CTVEA Offices

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

When an online account is created, or when a password or PIN is created or changed, CTVEA will mail a letter to customer's address of record notifying them of the change. When an email address of record is changed, CTVEA will send an email to customer's prior email address notifying them of the change. When a postal address of record is changed, CTVEA will mail a letter to customer's former postal addresses of record notifying them of the change. Each of the notices provided under this paragraph will not reveal the changed information and will direct the customer to notify CTVEA immediately if they did not authorize the change. Notwithstanding the foregoing, customer notice is not required for the creation of a PIN, password, or address of record established at the time that the customer initiates service, including during the installation visit.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any CTVEA employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the CTVEA CPNI Compliance Manager, and must not report or disclose such information 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 CTVEA'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 CTVEA'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 Manager.

If a CTVEA 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 CTVEA's CPNI Compliance Manager who will determine whether to report the incident to law enforcement. CTVEA's Compliance Manager will determine whether it is appropriate to update CTVEA's CPNI policies or training materials and/or take other action in light of any new information; the FCC's rules require CTVEA 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 CTVEA CPNI Compliance Manager 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, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450) for instructions.

CTVEA will not except as provided below notify customers or otherwise disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI, and will further defer such notification and disclosure upon the request of either agency. (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 CTVEA 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.

IV. RECORD RETENTION

The CTVEA Compliance Manager is responsible for assuring that we maintain 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.

CTVEA 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 disclose CPNI.

CTVEA maintains a record of all customer complaints related to CTVEA's handling of their CPNI, and records of CTVEA's handling of such complaints, for at least two years. The CPNI

Compliance Manager will assure that all complaints are reviewed and that CTVEA considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

CTVEA 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 CTVEA 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 explain how CTVEA'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

CTVEA 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 CTVEA'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, CTVEA 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 CSRs be cognizant that some unauthorized persons may have significant apparent familiarity with a customer's biographical and account information.