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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2016 covering the prior calendar year 2015

1. Date filed: February 12, 2016
2. Name of municipality covered by this certification: City of Elberton, Georgia d/b/a Elberton Utilities
3. Form 499 Filer ID: 827067
4. Name of signatory: Lanier Dunn
5. Title of signatory: City Manager
6. Certification:

I, Lanier Dunn, certify that I am an officer of the City of Elberton, Georgia, a municipality doing business as Elberton Utilities ("Elberton Utilities") and, acting as an agent of the city, that I have personal knowledge that Elberton Utilities 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 Elberton Utilities' procedures ensure that it 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.

Elberton Utilities has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. Elberton Utilities does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Elberton Utilities has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by Elberton Utilities at either the Georgia Public Service Commission, any court, 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.

Lanier Dunn

Lanier Dunn
City Manager
City of Elberton, Georgia
Executed February 11, 2016

CPNI Compliance Policies of City of Elberton, Georgia d/b/a Elberton Utilities

The following summary describes the policies of the City of Elberton, Georgia d/b/a Elberton Utilities ("City") 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."

This disclosure does not apply to the City's practices with respect to CPNI associated with its broadband Internet access services, which became subject to the requirements of Section 222 of the Communications Act effective June 12, 2015, but which are not subject to the FCC's CPNI rules. City is committed to engaging in reasonable, good-faith steps to protect broadband CPNI from unauthorized use or disclosure.

City's policy, administered by its CPNI Compliance Manager Lanier Dunn, the City Manager, establishes the procedures and safeguards regarding City's use and disclosure of CPNI set forth below.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

City 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 City, 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.

City does not use CPNI to market services. In the event that City later 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 the CPNI Compliance Manager. If such use is approved, City shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

City 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, City 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 City's existing policies that would strengthen protection of CPNI, they should report such information immediately to City's CPNI Compliance Manager so that City may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to City Requesting CPNI

City does not provide Call Detail Information to inbound callers. 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.

For CPNI other than CDI, prior to revealing any CPNI or account information to the caller, City requires an inbound caller to authenticate their identity through means that is appropriate for the information sought and which adheres to City's duty to safeguard CPNI.

B. Online Access

To access CPNI online, customer must enter a password that is established in accordance with the requirements herein.

When a customer submits a request for new telephone service, they must establish an email address that will serve as an address of record for their telephone account, and they must select an initial password that must be entered to obtain online access to the Customer's telephone account information online. The customer may later change their password online after logging into the account using the existing password.

At the time the password is established or changed, the customer is advised to select a password that does not consist of any significant portion of the customer's name, family names, account number, telephone number, street address, zip code, social security number, date of birth, other biographical or account information, or easily guessed words or strings of digits.

If a customer forgets their password, they may contact the City to request that their password be sent to their email address of record. Passwords are not provided over the phone.

If there are 3 or more consecutive failed attempts at access to an online account without an intervening successful login, the account will be locked to protect it from serial access attempts by an unauthorized person. To unlock an account, the customer must call Company and provide identifying information to request that the account be unlocked, at which time an email will be sent to the customer's email address of record with a new randomly-generated password.

Because this new password is randomly generated, it is not expected to consist of any significant portion of the customer's account or biographical information. If there is an unusual number of requests to unlock an account, Company may contact the customer's telephone number of record or address of record to verify that the unlock requests were authorized by the customer.

C. In-Person Disclosure of CPNI at City Offices

City may disclose a customer's CPNI to an authorized person visiting a City 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 address of record is created or changed, City will send a notice to customer's prior address of record notifying them of the change. When an online access password is changed, City will send a notice to customer's address of record notifying them of the change. These notifications are not required when the customer initiates service, such as the creation of their online account and selection of an initial password that is required as part of the initial service order. These notices will not reveal the changed information and will direct the customer to notify City immediately if they did not authorize the change.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any City employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the City CPNI Compliance Manager. 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 City'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 City's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

Nothing in this policy authorizes any employee to violate Georgia law. In the event of an apparent conflict between Georgia law and the FCC's CPNI requirements or the requirements of this policy, the City CPNI Compliance Manager will consult the City's legal counsel.

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 City 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 City's CPNI Compliance Manager who will determine whether to report the incident to law enforcement or take other appropriate action. City's Compliance Manager will determine whether it is appropriate to update City's CPNI policies or training materials in light of the new information; the FCC's rules require City 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 City 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. An 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.

City will not 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.)

If City 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.

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

IV. RECORD RETENTION

The CPNI Compliance Manager is responsible for assuring that City 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.

City 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. If City later changes its policies to permit the use of CPNI for marketing, it will maintain a record, for at least one year, of supervisory review of marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI.

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

City will have the City Manager, as its authorized officer and agent, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that City 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 Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how City'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. Any confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

All City employees with access to CPNI receive a summary of City'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.