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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2015 covering the prior calendar year 2014

1. Date filed: March 2, 2015

2. Name of companies covered by this certification:

MCC Telephony, LLC and operating subsidiaries:

MCC Telephony of Florida, LLC
Mediacom Telephony of Illinois, LLC
MCC Telephony of Missouri, LLC
MCC Telephony of Minnesota, LLC
MCC Telephony of Georgia, LLC
MCC Telephony of Iowa, LLC
MCC Telephony of the Mid-Atlantic, LLC
MCC Telephony of the West, LLC
MCC Telephony of the Midwest, LLC
MCC Telephony of the South, LLC

3. Form 499 Filer ID: 825517

4. Name of signatory: Daniel Templin

5. Title of signatory: President

6. Certification:

I, Daniel Templin, certify that I am an officer of MCC Telephony, LLC and its operating subsidiaries listed above (together, "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 access to or release of CPNI. Company 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. Company has therefore 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.

Daniel Templin
President
MCC Telephony, LLC
MCC Telephony of Florida, LLC
Mediacom Telephony of Illinois, LLC
MCC Telephony of Missouri, LLC
MCC Telephony of Minnesota, LLC
MCC Telephony of Georgia, LLC
MCC Telephony of Iowa, LLC
MCC Telephony of the Mid-Atlantic, LLC
MCC Telephony of the West, LLC
MCC Telephony of the Midwest, LLC
MCC Telephony of the South, LLC

Executed March 2, 2015

PUBLIC VERSION

Customer Proprietary Network Information Policy of MCC Telephony

Effective December 8, 2007

Federal law governs the use of Customer Proprietary Network Information ("CPNI"). MCC Telephony, LLC f/k/a MCC Telephony, Inc.; MCC Telephony of Florida, LLC; MCC Telephony of Illinois, LLC; MCC Telephony of Missouri, LLC; MCC Telephony of Minnesota, LLC; MCC Telephony of Georgia, LLC; MCC Telephony of Iowa, LLC; MCC Telephony of the Mid-Atlantic, LLC; MCC Telephony of the West, LLC; MCC Telephony of the Midwest, LLC; and MCC Telephony of the South, LLC (collectively, "MCC" or the "Company") uses and safeguards CPNI in accordance with federal law, including the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*., as applied to its interconnected VoIP telephone service and as stated in this policy.

Federal law defines CPNI as:

- Information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by a customer of a telecommunications carrier, and is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

- Information contained in the bills pertaining to a telephone exchange service or telephone toll service received by a customer of a carrier.[1]

For example, CPNI includes information such as the type of services to which the customer subscribes and the customer's use of those services (*e.g*., call patterns, call volume, etc.). CPNI does not include information derived from non-telecommunications services offered to the customer.

MCC's policy, administered by its CPNI Compliance Supervisor Anna Sokolin-Maimon, establishes the procedures and safeguards regarding MCC's use and disclosure of CPNI set forth below.

Because the details of this policy could provide a roadmap for unauthorized persons to attempt to subvert these policies and attempt to obtain CPNI, copies of this policy and related training materials are classified as confidential and may be provided only to MCC employees or to parties approved by the CPNI Compliance Supervisor. [REDACTED]

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Under federal law, absent customer approval, MCC is permitted to use, disclose, or permit access to CPNI only as follows:

[1] *See* 47 U.S.C. § 222(h)(1)(A), (B).

(1) in its provision of the communications service from which such information is derived and for services necessary to, or used in, the provision of such communications service, including the publishing of directories;

(2) to protect our rights and property, our customers, and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, our services;

(3) to provide or market service offerings among the categories of service to which the customer already subscribes;

(4) to provide inbound marketing, referral or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of the carrier's use to provide such service. In requesting such approval, the Company representative must explain that the customer has a right, and that Company has a duty, under federal law, to protect the confidentiality of CPNI; specifies the types of CPNI that would be used for the call and the purposes for which it would be used; informs the customer of his or her right to decline such use and that such denial will not affect the provision of any services to which the customer subscribes; and will not attempt to encourage a customer to freeze third-party access to CPNI;

(5) to provide inside wiring installation, maintenance, or repair services;

(6) to initiate, render, bill and collect for voice or telecommunications services; or

(7) as required by law.

MCC does not use CPNI for outbound marketing of services to customers that are outside of the category of services to which the customer does not already subscribe. MCC does not share CPNI with affiliates or third parties for marketing purposes, and does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. MCC may engage third parties to assist in billing and collections, administration, surveys, marketing, service delivery and customization, maintenance and operations, and fraud prevention.

All marketing campaigns must receive prior supervisory approval and must be conducted in accordance with this policy. If MCC seeks to use CPNI to market services to customers outside of the category of services to which the customer subscribes, then MCC will first modify its CPNI policies to incorporate the FCC's rules pertaining to seeking and obtaining customer approval for the use of CPNI.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, MCC 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 MCC's existing policies that would strengthen protection of CPNI, they should report such information immediately to

MCC's CPNI Compliance Supervisor so that MCC may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls Requesting CPNI

CSRs are trained to require an inbound caller to authenticate their identity prior to revealing any CPNI to the caller. [REDACTED]

Notwithstanding the above, MCC does not provide Call Detail Information (CDI) 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. Requests for CDI are handled in accordance with the following procedures:

[REDACTED]

B. Online Access

To access MCC's online portal that provides access to CPNI, the customer must enter a login ID that they create and a password established in accordance with the criteria set forth below.

[REDACTED]

C. In-Person Disclosure of CPNI at MCC Offices

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

It is MCC's policy that when an online account is created, or when a password is created or changed, MCC will send a notice to customer's address of record notifying them of the change, and that when an address of record is changed, MCC will send a notice to a preexisting customer address 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 MCC immediately if they did not authorize the change. These notifications are not required when the customer initiates service.

III. TRAINING

All employees receive a copy of MCC'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, all CSRs, personnel at retail

offices that may receive requests for CPNI, and marketing personnel receive additional training as to when they are, and are not, authorized to use CPNI. [REDACTED]

IV. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

MCC employees have been informed that should an employee become aware of any potential breach of data security which may involve CPNI, that person is to notify a designated individual in the legal department of the Company. MCC employees are prohibited from notifying their customers of the potential beach unless and until directed to do so by the legal department.

Any MCC employee that becomes aware of any breaches, suspected breaches or attempted breaches of CPNI or other personally identifiable customer account information must report such information immediately to the MCC CPNI Compliance Supervisor, 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.

MCC's CPNI Compliance Supervisor is Anna Sokolin-Maimon, [REDACTED].

It is MCC'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 MCC'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 whether that incident would constitute a breach under this definition, the incident must be reported to the CPNI Compliance Supervisor.

If an MCC 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 MCC's CPNI Compliance Supervisor who will determine whether to report the incident to law enforcement and/or take other appropriate action. MCC's Compliance Supervisor will determine whether it is appropriate to update MCC's CPNI policies or training materials in light of any new information.

B. Notification Procedures

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the MCC CPNI Compliance Supervisor 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.

MCC will not under any circumstances notify customers or disclosing 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 MCC 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. MCC will delay notification to customers or the public upon request of the FBI or USSS.

If the MCC Compliance Supervisor 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 disclosure; MCC still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

V. RECORD RETENTION

MCC will maintain for at least two years: (1) 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; and (2) a record of all customer complaints related to MCC's handling of CPNI, and records of MCC's handling of such complaints. The CPNI Compliance Supervisor will assure that all complaints are reviewed and that MCC considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

MCC will maintains a record, for a period of at least one year, of: (1) those limited circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI; (2) of supervisory review of outbound marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI; and (3) its sales and marketing campaigns that use its customers' CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, and the products and services offered as a part of the campaign; and (4) records associated with customers' approval or non-approval to use CPNI, and of notification to customers prior to any solicitation for customer approval of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

MCC 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 MCC 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 MCC'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. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.