

DO NOT FILE COPY ORIGINAL

LTS OF ROCKY MOUNT, LLC
3801 SUNSET AVENUE
P.O. BOX 7009
ROCKY MOUNT, NORTH CAROLINA 27804

Received & Inspected

JAN 26 2009

FCC Mail Room

January 14, 2009

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Dear Federal Communications Commission:

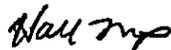
RE: EB Docket No. 06-36 Certification of CPNI Filing (2009)

Enclosed: 1 original and 4 copies sent to Ms. Dortch

- The following has been sent 2 copies of this certification and statement via USPS:
Federal Communications Commission
Enforcement Bureau
Telecommunications Division
445 12th Street, SW.
Washington, D.C. 20554
- The following has been sent 1 copy of this certification and statement via USPS:
Best Copy and Printing, Inc.
Portals II
445 12th street, S.W., Room CY-B402
Washington, DC 20554

Enclosed is LTS' certificate of compliance and statement explaining how LTS' operating procedures ensure compliance with the rules. If I can provide any additional information, or if you prefer this information in a different format, please let me know. My address is above, and my direct office is 252-451-2037).

Sincerely,



Hall Thorp
Manager

Enclosures

No. of Copies rec'd 0 + 4
List A B C D E

EB Docket 06-36

JAN 26 2009

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2009

Date filed: January 14, 2009

LTS of Rocky Mount, LLC

Form 499 Filer ID: 825617

Name of signatory: Hall Thorp

Title of signatory: Manager

I, Hall Thorp, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.

Attached to this certification is an accompanying statement explaining how LTS of Rocky Mount's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

LTS of Rocky Mount, LLC has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

LTS of Rocky Mount, LLC has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g. instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

Hall Thorp

LTS of Rocky Mount LLC's Operating Procedures to ensure compliance with CPNI

LTS of Rocky Mount, LLC is relatively small non-facilities based CLEC in North Carolina and Virginia. LTS provides prepaid residential telephone service only, and provides long distance to customers via a third party. LTS's operating procedures used to ensure compliance with proprietary customer information is as follows.

LTS operations to ensure compliance with CPNI comes from two perspectives: 1) authorized access to customer information (i.e. information that would be transferred voluntarily to another party), and 2) unauthorized access to customer information (i.e. information that would be stolen by another party whether physically or electronically).

1. Since inception, it has been the policy of LTS never to transfer customer information without express knowledge by relevant regulatory authorities. To ensure this:
 - a. Verbal instruction to all Customer Service Representatives ("CSRs") to confirm identity of customer, and only discuss one account on any given in-coming or out-going call. In addition, only provide information about a given account that is pertinent to that account (i.e. due date, amount due, etc...).
 - b. Unannounced weekly audits of CSR communications (i.e. monitoring) is performed to ensure quality and compliance.
 - c. Per LTS' Operating Agreement, management of LTS is precluded from purchasing or selling tangible or intangible assets of the organization (i.e. billing records), without express approval of the members. This organizational safeguard prohibits the sale of customer information by Management.

2. LTS utilizes a billing system that is kept physically and electronically secure:
 - a. All CSRs are instructed to shred any paper related to a customer's account.
 - b. All hard-copies of Customer Service Agreements are kept in secure storage inside our corporate office (alarm system, file cabinets locked, etc...). Any Agreements that are moved to secure storage are kept locked and then shredded after a period of 3 years.
 - c. All electronic customer information is kept secure under a triple-redundancy system, wherein the Managing Partner, Chief Operating Office, and Programmer may only transfer files (i.e. amount of long distance minutes used during a month that is sent to the long distance provider) with the express approval and authority of these three people. In addition, all customer information is stored on a segregated internal network, which is not accessible externally.
 - d. All customers are sent a monthly statement. This mailing is performed in-house, and customer records are not transmitted to any third party for mailing.

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

Received & Inspected

JAN 26 2009

EB Docket 06-36

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2008

Date filed: January, 2009

Name of company(s) covered by this certification: Comspan Communications, Inc.

Form 499 Filer ID: 822642

Name of signatory: Michelle Elkins

Title of signatory: Regulatory Admin.

I, Michelle Elkins, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 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 set forth in section 64.2001 et seq. of the Commission's rules [attach accompanying statement].

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed Michelle Elkins [signature]
Michelle Elkins

No. of CPNI records: 044
List A B C D

INDEX

- 1.1 Purpose of Document**
- 2.1 Comspan Communications compliance policy and process**
- 3.1 FCC Ruling**

1.1 Purpose of Document

The purpose of the ComSpan CPNI Document is for the implementation and compliance to the Federal Government ruling of CPNI.

2.1 ComSpan Communications will require all employees to comply with the CPNI rulings.

ComSpan CSR's will validate all callers *before* offering any information or service assistance. There will be no exceptions to the rule. All customers will be validated as an authorized contact. The authorized contact may add an additional contact with verifiable information (IE: a SS# or password) at any time.

Customers Authentication can be any of the following:

If the call is customer initiated, password protection can be provided.

Customer may provide last four digits of SS # or Federal Tax ID#.

Customers entering the office, must provide a valid photo ID.

Carrier can mail call detail records to the customer's address of record.

If the customer selects to establish a password, the carrier must authenticate the customer without the use of readily available biographical information (e.g., customers social Security number, last 4 digits of SSN, mother's maiden name, home address, date of birth) or account information (e.g., telephone number associated with the account, account number, billed amount)

The password cannot be readily available biographical information.

If the password s changed, ComSpan Communications will mail a follow up notification to the customers billing address of record. (The communication will not include the new password)

ComSpan CSR's will begin immediately collecting data from all new and existing customers. A for customer verification and enter the information into the ComSpan billing system

3.1 FCC Ruling:

**FCC RULES ON CUSTOMER RETENTION & WINBACKS:
CITES & EXCERPTS**

Customer Proprietary Network Information (CPNI):

Order on Reconsideration and Petitions for Forbearance, FCC 99-223, CC Docket No. 96-149; Adopted August 16, 1999; Released September 3, 1999 (CPNI)

Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd. 8061, FCC 98-27, CC Docket No. 96-115, Adopted Feb. 19, 1998; Released Feb. 26, 1998 (CPNI I)

Slamming:

Corrected Version, First Order on Reconsideration, FCC 00-135, CC Docket No. 94-129; Adopted April 13, 2000; Released, May 3, 2000

Second Report and Order and Further Notice of Proposed Rulemaking, FCC 98-334, CC Docket No. 94-129; Adopted December 17, 1998; Released, December 23, 1998 (Slamming)

CUSTOMER RETENTION & VERIFICATION

Definition

Customer retention deals with the "soon-to-be-former" customer. CPNI, ¶74. "Retention marketing . . . refers to a carrier's attempts to persuade a customer to remain with that carrier before the customer's service is switched to another provider." CPNI, ¶64.

Use of CPNI Not Allowed for Retention

Carriers cannot use CPNI¹ to attempt to retain a customer "during the time subsequent to the customer's placement of an order to change carriers and prior to the change actually taking place." CPNI, ¶69.

¹CPNI includes, among other things, to whom, where and when a customer places a call, as well as the types of service offerings to which the customer subscribes and the extent the service is used. CPNI means the 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. CPNI also includes information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

A carrier cannot “use CPNI to retain soon-to-be-former customers where the carrier gained notice of a customer’s imminent cancellation of service through the provision of carrier-to-carrier service.” CPNI, ¶76.

“[C]ompetition is harmed if *any* carrier uses carrier-to-carrier information, *such as switch or PIC orders*, to trigger retention marketing campaigns.” CPNI, ¶76 (emphasis added).

Carrier change information is proprietary. CPNI, ¶77. The carrier executing a change is “prohibited from using such information to attempt to change the subscriber’s decision to switch to another carrier.” *Id.* (citing Slamming, ¶106). “Thus, where a carrier exploits advance notice of a customer change by virtue of its status as the underlying network-facilities or service provider to market to that customer, it does so in violation of” the law. CPNI, ¶77.

Verification Not Allowed: “Interference with the Execution Process”

“[P]ermitting executing carriers to verify independently carrier changes that have already been verified by submitting carriers could have anticompetitive effects. . . . [E]xecuting carriers would have both the incentive and the ability to delay or deny carrier changes, using verification *as an excuse*, in order to benefit themselves or their affiliates. . . . Therefore, . . . the executing carrier may *only* use such information to provide service to the submitting carrier, i.e., changing the subscriber’s carrier, and *may not attempt to verify* that subscriber’s decision to change carriers.” Slamming, ¶99 (emphasis added); *see also* CPNI, ¶83.

“An executing carrier shall not verify the submission of a change in a subscriber’s selection of a provider of telecommunications service received from a submitting carrier. For an executing carrier, compliance with the procedures prescribed in this part shall be defined as prompt execution, without any unreasonable delay, of changes that have been verified by a submitting carrier.” Slamming, 64.1120(a)(2).

“[W]e require carriers to provide parity in executing carrier changes for competitors and promptness in executing carrier changes generally.” Slamming, ¶103.

“[W]e expect carriers to fulfill subscriber requests as quickly as possible, using the most technologically efficient means available to implement changes to subscribers’ telecommunications services. Noncompliance with this standard could be considered unreasonable delay.” Slamming, ¶105.

“A party that believes that a carrier is delaying execution of carrier changes . . . should file a complaint in the appropriate forum.” Slamming, ¶103.

"[A] carrier's failure to disclose CPNI to a competing carrier that seeks to initiate service to a customer who wishes to subscribe to a competing carrier's service may well constitute an unreasonable practice in violation of section 201(b), depending on the circumstances." CPNI, ¶89.

WINBACK/REGAINING OF CUSTOMER

Definition

"Regaining a customer applies to marketing situations where a customer has *already switched to and is receiving service* from another provider." CPNI, ¶64 (emphasis added).

When Allowed

Carriers are "able to use CPNI to engage in winback marketing campaigns to target valued former customers that have switched to other carriers." CPNI, ¶65.

"Customers expect carriers to attempt to win back their business by offering better-tailored service packages, and that such precise tailoring is most effectively achieved through the use of CPNI." CPNI, ¶68.

When Limited

Carriers may use CPNI of former customers "*to market the same category of service* from which CPNI was obtained to that former customer." CPNI, ¶65 (emphasis added). "Customers expect that CPNI generated from their entire service will be used by their carrier to market improved service within the parameters of the customer-carrier relationship. . . . Under the total services approach, the customer's implied approval is limited to the parameters of the customer's" *same category of service*. CPNI I, ¶24, as modified by CPNI ¶67.

"An important limitation . . . is that the carrier may use CPNI of the former customer to offer that customer *the service or services to which the customer previously subscribed*. It would be inconsistent with the *total services approach* for a carrier to use such CPNI to offer new services outside the former customer-carrier relationship." CPNI, ¶72 (emphasis added).

"Under the total service approach, for example, a carrier whose customer subscribes to service that includes a combination of local and CMRS would be able to use CPNI derived from this entire service *to market to that customer all related offerings, but not to market long distance service to that customer*, because the customer's service excludes any long distance component. Thus, under the total service approach, the carrier's permitted use of CPNI reflects the level of service subscribed to by the customer from the carrier." CPNI I, ¶30 (emphasis added)

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

Annual 64.2009(e) CPNI Certification for 2008

Date filed: **January 15, 2009**

Name of Company covered by this certification: **88 Telecom Corporation**

Form 499 filer ID: **825362**

Name of Signatory: **Gang Zhao**

Title of Signatory: **President**

Received & Inspected

JAN 26 2009

FCC Mail Room

I, **Gang Zhao**, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 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 set forth in section 64.2001 et seq. of the Commission's rules.

The company has taken actions to against data brokers in the past year:

1. 88 Telecom did not sell, lease or otherwise distribute customer names or usernames to third parties. Information collected from our customers will not be shared with, nor divulged to, any other party, unless required by court order or subpoenaed by a law enforcement agency.
2. 88 Telecom did not use a customer's information for marketing services to customers that are outside of the category of service to which the customer has not already subscribed. 88 Telecom does not share CPNI with affiliates or third parties for marketing purposes.
3. 88 Telecom may engage third parties to assist in billing and collections, administration, surveys, marketing, service delivery and customization, maintenance and operations, and fraud prevention.
4. If 88 Telecom seeked to promote services to customers outside of the category of services to which the customer subscribes, then 88 Telecom would notify customer at that time of their right to choose not to be a part of any such marketing campaign.
5. All marketing campaigns must receive prior approval and must be conducted in accordance with the CPNI policy.
6. All 88 Telecom employees have been trained as when they are, and are not, authorized to use CPNI. 88 Telecom will take any necessary disciplinary action to prevent violation of this policy.
7. 88 Telecom had a corporate officer who acts as agent for the company and signs a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has maintained operating procedures that are adequate to ensure compliance with applicable CPNI rules. 88 Telecom provides a statement that accompanies this certificate verifying the compliance.

No. of Copies rec'd 044
List A B C D E

The company has not received any customer complaints in the past year concerning any breach activities of CPNI.

Signature: 

Title: president

CPNI Rules Compliance Statement

Date: January 15, 2009

From: 88 Telecom Corporation
2525 Van Ness Ave. #222
San Francisco, CA 94109

To: Federal Communications Commission
445 12th St., Suite TW-A325
Washington, DC 20554

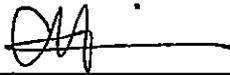
ATTN: the Commission's Secretary/ Marlene H. Dortch

To Whom It May Concern:

I have examined all the procedures, documents, files and records of 88 Telecom Corporation as required under the FCC's CPNI Rules, 47 C.F.R : 64.2009(e). In my understanding and to the best of my knowledge, according to the examination carried out by me and the explanation furnished to me by 88 Telecom's officers and agents, I hereby certify that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules, in respect of the aforesaid calendar year 2008.

Respectfully submitted 2525 Van Ness Ave. #222, San Francisco, CA 94109 by,

Charlie Zhao/ President of 88 Telecom



Signature of Agent

Date: 1/15/2009



Privacy on this site

<http://www.88card.com/privacy.asp>

What personally identifiable information is collected on this site?

Visitors may supply personally identifiable information (such as name, address or telephone numbers) for various purposes on this site. These purposes include registering to receive e-mail newsletters, requesting further information about our products, or simply asking a question about 88card.com. We do not collect personal information from you unless you provide it to us. This means that you can visit our site without telling us who you are or revealing any personally identifiable information about yourself.

How is it used?

88 Telecom is committed to protecting the privacy of its customers. We do not sell, lease or otherwise distribute customer names or usernames to third parties. Information you give us will not be shared with, nor divulged to, any other party, unless required by court order or subpoenaed by a law enforcement agency.

When you supply information about yourself for a specific purpose, we use the information for only that purpose (such as to provide the service or information you have requested). For example, you may be asked to give us individual information to receive information, manage online services, or apply for a job.

Should any material changes be made to the ways in which we use personally identifiable information, we will take commercially reasonable measures to obtain e-mail consent from you. We will also post the changes to our use of personally identifiable information on our site at least 30 days prior to a change.

Security

Personally identifiable information is stored on our Web server and is not publicly accessible. Further, personally identifiable information is only accessed by our employees on a "need to know" basis. All our employees must go through privacy training upon starting with us. We meet or exceed all industry standards for the protection of personally identifiable information.

Please note: When you order a card online and enter your payment information, you can't access it right away. We have to call you back to verify your information before we activate the pin. That is for your protection.

We can't release call detail information based on customer-initiated telephone contact, except one of the conditions has been met: (1) When a customer provides a pre-established password; (2) when a customer requests that the information be sent to his/her address of record; or (3) when we call the telephone number of record and discloses the information.

Choice/Opt-out

If you have registered to receive e-mail communications from us and later change your mind, you may contact us to have your name removed from our distribution lists. You can send an e-mail to support@88card.com or mail us at: 2525 Van Ness Ave. #222, San Francisco, CA 94109.

Correct/Update

If you would like to verify the data we have received from you or to make corrections to it, you may contact us either by e-mail or mail address provided above.

Does this site use cookies?

88card.com does not use cookies.

Links

This site may contain links to other Web sites. Please note that when you click on one of these links, you are entering another site. We encourage you to read the privacy statements of these linked sites as their privacy policy may differ from ours.

E-mail Links

We use e-mail links located on this site to allow you to contact us directly via e-mail. We use the information provided in your e-mail to respond to your questions or comments. We may also store your comments for future reference. Your personal information is only shared with third parties with your explicit permission.

Legal Disclaimer

We may disclose personal information when required by law or in the good-faith belief that such action is necessary in order to conform to the edicts of the law or comply with legal process served on 88card.com.

Customer Proprietary Network Information Policy

Federal law governs the use of Customer Proprietary Network Information ("CPNI"). 88 Telecom uses CPNI in accordance with federal law and as stated in this policy.

Federal law defines CPNI as:

The individually identifiable information that is created by a customer's relationship with a communications provider, such as data about the frequency, duration and timing of calls, the information on a customer's bill and call-identifying information.

For example, CPNI includes information such as the type of services that the customer subscribes to 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. Under federal law, absent customer consent, 88 Telecom is permitted to use, disclose, or permit access to CPNI as follows:

- (1) to protect our rights and property, our customers, and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, our services;
- (2) to provide or market service offerings among the categories of service to which the customer already subscribes;
- (3) for the provision of customer premises equipment;
- (4) for billing and rendering services to the customer; and
- (5) as required by law, such as in response to a validly issued subpoena.

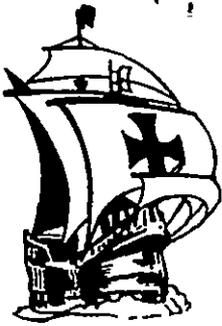
88 Telecom does not use CPNI to market services to customers that are outside of the category of service to which the customer does not already subscribe. 88 Telecom does not share CPNI with affiliates or third parties for marketing purposes. 88 Telecom may engage third parties to assist in billing and collections, administration, surveys, marketing, service delivery and customization, maintenance and operations, and fraud prevention. If 88 Telecom seeks to market services to customers outside of the category of services to which the customer subscribes, then 88 Telecom will notify customer at that time of their right to choose not to be a part of any such marketing campaign. All marketing campaigns must receive prior approval and must be conducted in accordance with this policy.

All employees will be trained as to when they are, and are not, authorized to use CPNI. 88 Telecom will take any necessary disciplinary action for violation of this policy.

88 Telecom has a corporate officer who acts as agent for the company and signs a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with applicable CPNI rules. 88 Telecom provides a statement that accompanies this certificate explaining that its operating procedures are adequate to ensure compliance with CPNI regulations.

For more information

If you have any questions, concerns or comments, please e-mail support@88card.com.



DOCKET FILE COPY ORIGINAL

COLUMBUS TELEPHONE COMPANY

Destination Excellence I

224 South Kansas Avenue • Columbus, Kansas 66725

President - Ronald Boulware
Vice-President - Wes Houser
Treasurer - Larry Prauser
Secretary - Patricia Carroll
Director - Paul Schmidt
Director - David Soper
Director - Evan McNemar
General Manager - [unclear]

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

EB Docket 06-36

Received & Inspected

JAN 26 2009

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2008

Date Filed: January 20, 2009

Name of company covered by this certification: Columbus Telephone Company

Form 499 Filer ID: 805716

Name of signatory: Patricia Carroll

Title of signatory: Corporate Secretary

I, Patricia Carroll, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. Section 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g. instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed [Signature] [electronic signature if applicable]

No. of Copies rec'd 0+4
List A B C D E

Received & Inspected

JAN 26 2009

FCC Mail Room

***CUSTOMER PROPRIETARY NETWORK
INFORMATION***

CPNI

***OPERATING PROCEDURE
GUIDELINES***

COLUMBUS TELEPHONE CO.

EFFECTIVE 12-08-07

Summary Overview of CPNI Operating Procedures of Columbus Telephone Co.

- CPNI effective operations date: December 8, 2007
- CPNI is Call Detail Records (CDR's), Account information relating to customer service relationship
- Designated Compliance Officer: General Manager
- Backup Compliance Officer: Corporate Secretary
- Training Requirements: Each March, the General Manager and/or the Corporate Secretary will hold a training session on CPNI. All persons receiving training will certify attendance at said training.
(See Attached)
- Columbus Telephone Co. will not utilize the "One-Time", password approach to "authenticate a customer. We will ask the for bill detail (services they subscribe to, amount of last months bill, other name's on the account etc.) Then we will call the customer back at the telephone number of record. We will also ask the customer a question with the answer entered into the customer account record for future use.
- Columbus Telephone Co. will notify customers immediately of changes to their accounts, specifically: a password, a backup or forgotten password, an online account, or address of record. This notification will be made in the form of written correspondence, mailed to the person(s) of record on the account, at the account billing address.

- **Disciplinary Procedure:** In the event of a breach of CPNI rules by an employee of Columbus Telephone Co., the following actions will occur;
 - First offense: A verbal reprimand will be given.
 - Second offense: A written reprimand will be given with a copy to the personnel file.
 - Third offense: Dismissal.

- We will only provide CPNI to the person of record on the account.

Suggested Procedure: For In-Office Customer Visit and Customer Initiated Calls

In-office Customer Visit

- Step 1.** Authenticate the customer with a valid photo ID and confirm that the person is listed as a contact on the account.
- Step 2** Check status of customer's CPNI approval.
- Step 3:** Respond to the customer's request following the rules for whether or not CPNI approval is needed.

NOTE:

If the customer is just dropping off payment, no authentication is needed unless the customer needs to know the amount of the bill.

If the person paying the bill is not listed on the account, the company cannot disclose the amount due. The person would need to tell the company the amount that the customer wanted to pay on the account.

Customer- Initiated Call

- Step 1:** Authenticate the customer (password or authentication question, whichever your company has decided to use) and confirm that the customer is listed as a contact on the account.
- Step 2:** Check status of the customer's CPNI approval.
- Step 3:** Respond to the customer's request following the rules for whether or not CPNI approval is needed.

The company has made the decision not to issue passwords. A customer calls the office, and an answer to the authentication question has not been previously established. How should this be handled?

Apologize to the customer for the inconvenience. Explain to the customer, that to protect the customer's privacy, the FCC now requires the company to authenticate the customer before discussing any information in the account.

Since this does not involve authentication for a password, the CSR could do one of the following:

- Call the customer at the telephone number of record.
- Ask the customer to provide some information contained in the account, e.g., services the customer subscribes to, amount of last bill, other names listed on the account, etc.

Once the CSR has authenticated the customer, explain that whenever the customer calls the office in the future, you will ask them for the answer to a specific question that you are now going to ask. You will then need to ask the question and record the answer in the customer's account records.

EMPLOYEE CPNI TRAINING CERTIFICATION

On an annual basis an officer of our company must certify to the Federal Communications Commission (FCC) it has established procedures adequate to ensure compliance with the FCC's Customer Proprietary Network Information (CPNI) rules.

One of the things the officer is certifying to its employees, especially those having access to CPNI, have been trained on the CPNI rules. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the company is using for both call detail and non-call detail information.

By signing below, I acknowledge:

- I have received the required training on the CPNI rules.
- I understand the company's procedures for protecting CPNI.
- I understand the company's disciplinary process if I use CPNI inappropriately.
- I understand if I have any questions at any time regarding the rules, I should immediately contact the General Manager or Corporate Secretary.

Employee Printed Name: _____

Employee Signature: _____

Date: _____

RELEASE AUTHORIZATION AND INDEMNITY AGREEMENT

The undersigned jointly and severally agree to indemnify and save harmless Columbus Telephone Co., (Indemnitee) from any claim, action, liability or suit, arising from the following:

The release of Customer Proprietary Information (CPNI) on telephone number _____ to _____
(Name)

(Address)

(Telephone number)

In the event of any asserted claim, the Indemnitee shall provide the undersigned timely notice of same, and thereafter the undersigned shall at its own expense defend and protect Indemnitee against said claim.

In the further event the undersigned shall fail to so defend, then in such instance the Indemnitee shall have full rights to defend, pay or settle said claim with full rights of recourse against the undersigned for all fees, costs, expenses and payments made or agreed to be paid to discharge said claim.

This agreement shall be binding upon and inure to the benefit of the parties, their successors, assigns and personal representatives.

Signed under seal this _____ day of _____, 20__ .

Witness

Customer of Record Signature

Printed Name

Address

City

DOCKET FILE COPY ORIGINAL

Irvine Community Television, Inc.

251 Broadway, PO Box 186, Irvine KY 40336-0186 606-723-4240 or 606-723-3668

January 16, 2009

Received & Inspected

JAN 26 2009

FCC Mail Room

Secretary of Commission
Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street SW, Suite TW-A325
Washington, DC 20554

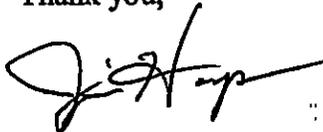
RE: EB Docket No. 06-36

Ms. Dortch

Enclosed are one original & 4 copies of the annual CPNI Compliance Certificate for 2008 including the Statement Regarding CPNI Operating Procedures by Irvine Community Television, Inc.

Please direct any questions to me at the above address or telephone or via email to jhays@irvineonline.net.

Thank you,



Jim Hays
Executive Vice-President
Irvine Community Television, Inc.

Enclosures (5): CPNI Compliance Certificate

No. of Copies rec'd 044
List A B C D E

JAN 26 2009

FCC Mail Room

CPNI COMPLIANCE CERTIFICATE

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: January 16, 2009

Name of company covered by this certification: Irvine Community Television, Inc. ("Irvine Community Television")

Form 499 Filer ID: 826866

Name of signatory: Jim Hays

Title of signatory: EVP

I, Jim Hays, certify that I am EVP of Irvine Community Television, and acting as an agent of Irvine Community Television, that I have personal knowledge that Irvine Community Television has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification as Attachment 1 is an accompanying statement explaining how Irvine Community Television's procedures ensure that Irvine Community Television is in compliance with the requirements set forth in Section 64.2001 *et seq.* of the Commission's rules.

Irvine Community Television has not taken any actions against data brokers in the past year.

Irvine Community Television has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed: _____



**ATTACHMENT 1
TO CPNI COMPLIANCE CERTIFICATE**

Statement Regarding CPNI Operating Procedures

Irvine Community Television's written CPNI Operating Procedures ensure that Irvine Community Television will be in compliance with 47 U.S.C. § 222 and the rules contained in the Title 47, Chapter 1, Subchapter B, Part 64, Subpart U of the Code of Federal Regulations. Included among the provisions of Irvine Community Television's CPNI Operating Procedures are:

- A requirement that Irvine Community Television have at all times a CPNI Compliance Supervisor to supervise the implementation of Irvine Community Television's CPNI Operating Procedures.
- Detailed procedures for safeguarding CPNI, including procedures for customer authentication and password protection of CPNI.
- Detailed procedures for determining what type of customer approval is necessary for use, disclosure and access to CPNI.
- A requirement that the billing system records for customers' accounts allow the status of the customer's CPNI approval to be easily ascertained.
- A requirement that personnel be trained as to when they are and are not authorized to use CPNI.
- A written disciplinary process for misuse of CPNI.
- Detailed filing, notice and recordkeeping requirements.
- Detailed procedures to be followed in the event of a breach of CPNI.

Irvine Community Television does not use, disclose or allow access to CPNI for any purpose that would require customer approval under 47 U.S.C. § 222 or the rules contained in the Title 47, Chapter 1, Subchapter B, Part 64, Subpart U of the Code of Federal Regulations.

Date: January 21, 2008

Marlene H. Dortch

Office of the Secretary

Federal Communications Commission

445 12th Street, SW, Suite TW-A325

Washington, DC 20554

JAN 26 2009

FCC Mail Room

Re: EB Docket No. 06-36, Certification of CPNI Filing - Calendar Year 2008

Dear Ms. Dortch:

This letter serves as the below-named Company's "Certification of CPNI Filing for Calendar Year 2008", as ordered in EB Docket No. 06-36.

Company Name: Rockwell Cooperative Telephone Association

Address: 111 4th St. N., Rockwell, IA 50469

Form 499 Filer ID: 807087

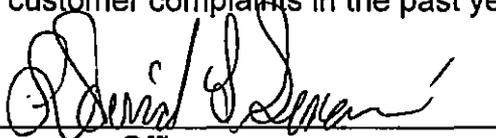
Name and Title of Signatory: David L. Severin, General Manager

I, David L. Severin, certify that I am an officer of the Company named above, and that, based on my personal knowledge and acting as an agent for the Company, the Company has established operating procedures that are adequate to ensure compliance with the rules established by the Federal Communications Commission ("FCC") concerning Customer Proprietary Network Information ("CPNI"), as set forth in Part 64, Subpart U, of the FCC's Rules and Regulations, 47 C.F.R. § 64.2001 *et seq.*, as revised.

The attached Statement demonstrates such compliance.

The Company has not taken any action (proceedings instituted or petitions filed by the Company at state commissions, the court system, or the FCC) against data brokers in the past year.

The Company has not received any customer complaints in the past year concerning unauthorized release of CPNI.



Company Officer

Dated: January 21, 2008

Attachment - Statement of Compliance

No. of Copies rec'd 0+4
List A B C D E

STATEMENT OF COMPLIANCE

The operating procedures of Rockwell Cooperative Telephone Association ensure compliance with the FCC's CPNI Rules.

USE OF CPNI IN MARKETING

Our company does not use CPNI in any of its marketing efforts, and does not permit the use of, or access to, customer CPNI by our affiliates or any third parties. We use, disclose or permit access to CPNI only for the purposes permitted under 47 U.S.C. Sections 222(c)(1) and (d).

CPNI SAFEGUARDS

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have an express disciplinary process in place if the rules are violated.

Our company establishes passwords with customers in order to authenticate customers. Authentication data does not rely on the customers' readily available biographical information.

Our company authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact or in-store visit.

Our company discloses call detail information (CDI) in a customer-initiated call only; after the customer provides a pre-established password; or, at the customer's request, by sending the CDI to the customer's address of record; or by calling back the customer at his or her telephone number of record.

Our company discloses CPNI to a customer in person at our retail location only when the customer presents a valid photo ID and the ID matches the name on the account.

Our company notifies a customer immediately of changes in: a customer's password, a customer's response to back-up means of authentication or address of record.

CPNI RECORDKEEPING AND REPORTING

Our company is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with the investigatory agency(ies), if we believe there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.



DOCKET FILE COPY ORIGINAL

Advanced Communications Technology

290 N. Brooks Box 7039 Sheridan, WY 82801

307.673.0910 Fax 307.673.0911 Email: act@actaccess.net

Received & Inspected

JAN 26 2009

FCC Mail Room

**CERTIFICATION OF CPNI FILING
[Section 64.2009(e) of FCC Rules]**

**EB-06-TC-060
EB DOCKET NO. 06-36**

I hereby certify that I am an Officer of Advanced Communications Technology, Inc.

I have personal knowledge that the Company and its affiliates established operating procedures that are designed to ensure compliance with the Customer Proprietary Network Information rules and requirements in Subpart U of Part 64 of the Federal Communications Commission's Rules (47 C.F.R. §§64.2001 through 64.2009). The attached Statement of CPNI Compliance explains how the Company's operating procedures ensure that it is in compliance with the foregoing FCC rules.

I am making this certification for the year 2008.

Signature

Michael S. Fox

Printed Name

Vice President/General Manager

Office Held

January 7, 2009

Date

No. of Copies rec'd 0
List A B C D E



Received & Inspected

JAN 26 2009

Advanced Communications Technology

FCC Mail Room 307.673.0910

290 N. Brooks Box 7039 Sheridan, WY 82801

Fax 307.673.0911 Email: act@actaccess.net

**Annual Report
Section 64.2009(e) of FCC Rules**

**EB-06-TC-060
EB DOCKET NO. 06-36**

- I. Actions taken against data brokers: None Reported
- II. Summary of Customer Complaints: None Reported
- III. Explanations of Breaches: None Reported
- IV. Explanations of Company Policies & Procedures for preventing unauthorized access to CPNI:

In October, 2007, the Range Family of Companies, which includes Advanced Communications Technology, Inc. adopted enhanced Corporate CPNI Policies and Procedures designed to protect our customers from actions by data brokers as well as prevent other unauthorized access to CPNI. Our manuals contain detailed procedures for our customer service representatives and other employees pertaining to the release of CPNI to customers and other authorized individuals. These manuals were designed to help all employees ensure the protection of our customers' information and include detail on disciplinary action for employees that intentionally or unintentionally fail to follow these procedures. In order to fully protect our customers, the Company believes that our CPNI Policy and Procedures Manuals fully comply with the minimum CPNI standards and rules as adopted by the Federal Communications Commission in its April 7, 2007 Order.

Further, it is Company policy that no CPNI will be used in any of its marketing campaigns. The Company's Compliance Officer will also ensure that no such protected information is used in any marketing effort.

Received & Inspected
JAN 28 2009
FCC Mail Room

DOCKET FILE COPY ORIGINAL

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: January 15, 2009

Name of company covered by this certification: Manawa Telephone Company, Inc.

Form 499 Filer ID: 0002-7194-74

Name of signatory: Thomas R. Squires

Title of signatory: President

I, Thomas R. Squires, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

Thomas R. Squires

No. of Copies rec'd 014
List ABCDE

Received & Inspected

JAN 28 2009

FCC Mail Room

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: January 15, 2009

Name of company covered by this certification: Manawa Telephone Company, Inc.

Form 499 Filer ID: 0002-7194-74

Name of signatory: Thomas R. Squires

Title of signatory: President

I, Thomas R. Squires, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed Thomas R. Squires



400 Pine Street, P.O. Box 8

Received & Inspected

LaMotte, Iowa 52054

Telephone: 563.773.2213 Facsimile: 563.773.2345 JAN 28 2009

www.lamotte-telco.com

FCC Mail Room

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: January 15, 2009

Name of company covered by this certification: LaMotte Telephone Company

Form 499 Filer ID: 801141

Name of signatory: Lynn Sanders

Title of signatory: President

I, Lynn Sanders, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the LaMotte Telephone Company, Inc. has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 47 C.F.R. § 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how LaMotte Telephone Company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

LaMotte Telephone Company does not use CPNI for marketing purposes. LaMotte Telephone Company does not sell or release CPNI to third parties for marketing purposes.

LaMotte Telephone Company has not taken any actions against data brokers in the past year. LaMotte Telephone Company is unaware of any pretexters whom are attempting to access CPNI. Steps taken to protect CPNI are outlined in the company's CPNI Policy and Procedures manual.

LaMotte Telephone Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed Lynn Sanders
Lynn Sanders, President
LaMotte Telephone Company
400 Pine Street, PO Box 8
La Motte, IA 52054
Telephone 563.773.2213
563.773.2345

No. of Copies rec'd 0
List ABCDE



400 Pine Street, P.O. Box 8

LaMotte, Iowa 52054

Telephone: 563.773.2213 Facsimile: 563.773.2345

www.lamotte-telco.com

Received & Inspected

JAN 28 2009

FCC Mail Room

LaMotte Telephone Company, Inc. (hereinafter referred to as "Company")
Certification of CPNI Filing
January 15, 2009

1. Company does not use CPNI for marketing purposes.
2. Company personnel are trained as to what information is classified as CPNI and do not use CPNI for marketing purposes.
3. Company and its employees carefully preserve the confidentiality of CPNI.
4. Company prohibits releasing call detail information or private information to customers during customer-imitated telephone contact except when the customer provides a password. If a customer does not provide a password, we prohibit the release of call detail information except by sending it to an address of record or by the Company personnel calling the customer at the telephone of record. We also require our staff to provide CPNI to customers based on in-store contact with valid photo ID.
5. Company requires its personnel to notify the customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed.
6. Company extended the application of the CPNI rules to VoIP customers.
7. Company has implemented appropriate safeguard policies for CPNI and has documented them in the Company's procedures for training personnel.
8. Company is submitting the CPNI Compliance Certificate in response to the Public Notice issued by the FCC on January 28, 2008, in DA-08-171 pursuant to 47 C.F.R. §64.2009(e), EB Docket No. 06-36.

Received & Inspected

JAN 28 2009

FCC Mail Room

DOCKET FILE COPY ORIGINAL

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: January 16, 2009

Name of company covered by this certification: Manawa Telecom, Inc.

Form 499 Filer ID: 0003-7461-38

Name of signatory: Thomas R. Squires

Title of signatory: President

I, Thomas R. Squires, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, e.g., instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

Thomas R. Squires

No. of Copies rec'd 014
List ABCDE

Received & Inspected

JAN 28 2009

FCC Mail Room

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date filed: January 15, 2009

Name of company covered by this certification: Manawa Telecom, Inc.

Form 499 Filer ID: 0003-7461-38

Name of signatory: Thomas R. Squires

Title of signatory: President

I, Thomas R. Squires, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed

Thomas R. Squires