

Consolidated

January 27, 2009

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

RE: EB Docket No. 06-36
Annual CPNI Certification for Year 2008

Dear Ms. Dortch:

In accordance with Public Notice DA 09-9, issued on January 7, 2009, attached is the annual CPNI certification filing for the year of 2008, pursuant to 47 C.F.R. § 64.2009(e), for Consolidated Telecom, Inc.

Sincerely,



Wendy Thompson Fast
President

Attachment

cc: Best Copy and Printing, Inc.
445 12th Street
Suite CY-B402
Washington, D.C. 20554

CPNIcomp.doc
1/27/2009 12:57:20 PM

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 27, 2009

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

Form 499 Filer ID: 809736

Name of signatory: Wendy Thompson Fast

Title of signatory: President

I, Wendy Thompson Fast, 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 against data brokers in the past year. If the Company obtains any information with respect to the processes pretexters are using to attempt to access CPNI, it will report that information along with what steps the Company is taking to protect CPNI.

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

Signed 

ATTACHMENT

OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

Consolidated Telecom, Inc. (the "Company") has implemented the following procedures to ensure that it is compliant with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), § 64.2001 through § 64.2011.

CPNI Manual

The Company has adopted a CPNI Manual that governs the use of CPNI by all Company employees, agents and independent contractors.

Compliance Officer

The Company has appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Company is in compliance with all CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training:

Employees are required to read the Company's CPNI Manual and attend a training session during which the Manual will be reviewed and discussed. The Compliance Officer arranges for the training on an annual basis, and more frequently as needed. Any new employee is trained when hired by the Company. 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. The training detail differs based on whether or not the employee has access to CPNI.

All employees are required to sign a CPNI Policy Acknowledgement. This Acknowledgement specifies that the employee has received a copy of the CPNI Manual, is responsible for reviewing and understanding the Manual and understands any violation of the Company's procedures will result in disciplinary action up to and including dismissal.

Employees are instructed that if they ever have any questions regarding the use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

Disciplinary Process

The Company has established a specific disciplinary process for improper use of CPNI. Disciplinary action is based on the type and severity of the violation and could include any of the following: counseling, retraining, reassignment, suspension or termination.

The disciplinary process is reviewed with all employees.

A copy of the Company's disciplinary process is kept in the CPNI manual.

Customer Notification and Request for Approval to Use CPNI

The Company has provided notification to its customers of their CPNI rights and has asked for customers' approval to use CPNI via the opt-out method. A copy of the notification is also provided to all new customers that sign up for service. Once customers deny the use of their CPNI, those decisions remain in force until changed. The company sends the opt-out notice every two years to those customers that have not previously opted out. When the opt-out mechanisms do not work properly to such a degree that consumers' ability to opt-out is compromised the Company will provide written notice to the FCC within five business days.

The status of a customer's CPNI approval is prominently displayed as soon as the customer's account is accessed. Employees can thus readily identify customers that have restricted the use of their CPNI.

A copy of the most recent opt-out notification is kept in the CPNI manual.

Marketing Campaigns

The Compliance Officer will review all marketing campaigns to ensure that materials are in compliance with CPNI rules. The campaign must be approved by the Compliance Officer.

The Company has a process for maintaining a record of any marketing campaign of its own, or its affiliates, that uses customers' CPNI.

Authentication

The Company does not disclose any CPNI until the customer has been appropriately authenticated as follows:

- In-office visit – The customer must provide a valid photo ID matching the customer's account information.
- Customer-initiated call – The customer is authenticated by providing an answer to a pre-established question and must be listed as a contact on the account.

If the customer wants to discuss call detail information that requires a password, the following guidelines are followed:

- If the customer can provide all of the call detail information (telephone number called, the time of the call, and the amount of the call) necessary to address the customer's issue, the Company will continue with its routine customer care procedures.
- If the customer cannot provide all of the call detail information to address the customer's issue, the Company will call the customer back at the telephone number of record, send the information to the address of record, or ask the customer to come into the office and provide a valid photo ID.

Notification of Account Changes

Whenever a change is made to the address of record, the Company promptly notifies customers by mailing a letter to the previous address of record. The Company has a process for tracking when a notification is required and for recording when and how the notification is made.

Notification of Breaches

Employees will immediately notify the Compliance Officer of any indication of a breach. If it is determined that a breach has occurred, the Compliance Officer will do the following:

- Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as practicable, but in no event later than seven business days after determination of the breach. The notification will be via the FCC link at <http://www.fcc.gov/eb/cpni>.
- Notify affected customers after seven full business days have passed since notification of the USSS and the FBI, unless the USSS or FBI has requested an extension.
- Notify affected customers or the public prior to seven days after the breach if there is an urgent need to avoid immediate and irreparable harm. Such notifications will be done only after consultation with the relevant investigating agency.

- Maintain a record of the breach, the notifications made to the USSS and FBI and the notifications made to customers. The record should include dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach and the circumstances of the breach.
- Include a summary of the breach in the annual compliance certificate filed with the FCC.

Annual Certification

The Compliance Officer will file a Compliance Certification with the FCC by March 1 of each year, for data pertaining to the previous calendar year.

Record Retention

The Company retains all information regarding CPNI. The minimum retention period for each type of record is as follows:

- CPNI notification and records of approval – one year
- Marketing campaigns – one year
- Breaches – two years
- Annual certification – five years
- Employee training certification – two years
- All other information – two years