Operating Procedures for Compliance with CPNI Rules

Consolidated Telephone Company, Consolidated Telco Inc., Consolidated Telecom Inc., Curtis Telephone Company and Consolidated Long Distance (the “Companies”) have 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 Companies have adopted a CPNI Manual that governs the use of CPNI by all Companies employees, agents and independent contractors.

**Compliance Officer**

The Companies have appointed a CPNI Compliance Officer. The Compliance Officer is responsible for ensuring that the Companies are 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 Companies 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 Companies. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and the authentication methods the Companies are 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 Companies 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 Companies have 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 Companies disciplinary process is kept in the CPNI manual.

**Customer Notification and Request for Approval to Use CPNI**

The Companies have provided notification to its customers of their CPNI rights and have 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.

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.

For the customers that have opted out and said the Companies cannot use their CPNI, that decision will remain valid until the customer changes it.

The Companies send the opt-out notice every two years to those customers that have not previously opted out.

The Companies will provide written notice to the FCC within five business days when the opt-out mechanisms do not work properly to such a degree that consumers’ ability to opt-out is more than an anomaly.

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 Companies have a process for maintaining a record of any marketing campaign of its own, or its affiliates, which uses customers’ CPNI.

**Authentication**

The Companies do 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, when it was called, and the amount of the call) necessary to address the customer’s issue, the Companies 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 Companies 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**

The Companies notify the customers of any changes that have been made to their account, by sending a notification to the previous address of record.  If the customer did not authorize any change, they are asked to contact our office immediately.

**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 customers only 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.

**Miscellaneous**

The Company's CPNI policies include reasonable measures to discover and protect against activity that is indicative of pretexting. Employees are instructed to notify the CPNI Compliance Officer if any such activity is suspected.

**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 Companies retain 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 – seven years
* Employee training certification – two years
* All other information – two years