

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

USConnect Holdings, Inc.

1000 Elm Street, Suite 1901, Manchester, NH 03101
603-622-0379

Date Filed: February 1, 2018

<u>Name of Company Covered by this Certification:</u>	<u>499 Filer ID</u>
CableCo, L.L.C.	824138
Dalton Telephone Company, Inc.	808972
Dalton Telecommunications, Inc.	827075
Elsie Communications, Inc.	808731
Livingston Telephone Company, Inc.	802017
Telcom Supply, Inc.	822916
The Rye Telephone Company	805392
S&A Communications, Inc.	826597
S&A Telephone Company, Inc.	804630
South Park, L.L.C. dba South Park Telephone Company	817360
Waverly Hall Communications, Inc.	827047
Waverly Hall Telephone Company, Inc.	807006

Name of signatory: Deborah Rand

Title of signatory: CEO

I, Deborah Rand, certify that I am an officer of the companies named above, and acting as an agent of the companies, that I have personal knowledge that the companies have 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 companies procedures ensure that the companies are in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The companies have not taken actions (*i.e.*, 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.

The companies have not received customer complaints in the past year concerning the unauthorized release of CPNI.

The companies represent and warrant that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The companies also acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: 

STATEMENT OF COMPLIANCE WITH CPNI RULES

USConnect Holdings, 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.

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 of the CPNI rules. The Compliance Officer is also the point of contact for anyone (internally or externally) with questions about CPNI.

Employee Training:

The Compliance Officer arranges for the training of all employees 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 detail of the training can differ based on whether or not the employee has access to CPNI.

After the training, all employees are required to sign a certification that they have received training on the CPNI rules, that they understand the Company's procedures for protecting CPNI and they understand the Company's disciplinary process for improper use of CPNI. Each employee is provided a CPNI manual for their review.

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. The disciplinary action is based on the type and severity of the violation and could include any or a combination of the following: retraining the employee on CPNI rules, notation in the employee's personnel file, formal written reprimand, suspension or termination.

The disciplinary process is reviewed with all employees.

A copy of the Company's disciplinary process is kept in the employee handbook.

Customer Notification and Request for Approval to Use CPNI

The Company provided "Opt Out" notification to its customers. If the customer does not object within the thirty (30) day waiting period, the customer is deemed to have consented to use of his/her CPNI. Regardless, the Company will not share the customer's CPNI with any joint venture partner, independent contractor or any other third party without customer affirmative express consent. For marketing purposes, the Company does mass marketing to all customers, or uses CPNI to market only service offerings among the categories of service to which the customer already subscribes.

If the Company receives a call from a customer who wants to discuss services outside of the customer's existing service offerings, the customer service representative uses the oral notification for one-time use of CPNI to obtain approval for the duration of the call only.

Marketing Campaigns

If the Company uses CPNI for any marketing campaign, the Compliance Officer will review the campaign and all materials to ensure that it is in compliance with the CPNI rules.

The Company has a process for maintaining a record of any marketing campaign of its own, or its affiliates, which 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 the CSR calling the customer back at their telephone number of record.

If the customer wants to discuss call detail information 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 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: 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 Company promptly notifies customers whenever a change is made to address of record. The notification to the customer will be mailed to the customer at their 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. The Subscriber Billing Program automatically generates a letter when a customer's address is changed. The letter is then mailed to the customer's previous address of record; a notation of the mailing is recorded in the billing program.

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 7 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 7 full business days have passed since notification to the USSS and the FBI, unless the USSS or FBI has requested an extension.
- If there is an urgent need to notify affected customers or the public sooner to avoid immediate and irreparable harm, it 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.

Summary of Consumer Complaints

There were no consumer complaints regarding unauthorized release of CPNI in the previous year.

Action against Data Brokers

There were no actions taken against data brokers or pretexters for unauthorized access to CPNI in the previous year.

Record Retention

The Company retains all information regarding CPNI in a CPNI file. Following is the minimum retention period we have established for specific items:

- 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