



1006 Twelfth Street • Aurora, Nebraska 68818  
voice 402.694.5101 • TTY 800.821.1834  
toll free 800.821.1831 • fax 402.694.2848  
e-mail: [info@hamiltonel.com](mailto:info@hamiltonel.com)  
website: [hamiltonel.com](http://hamiltonel.com)

February 16, 2018

Marlene H. Dortch, Secretary  
Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> Street, SW  
Washington, D.C. 20554

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

Dear Ms. Dortch:

Attached is the annual CPNI certification filing covering the year of 2017, pursuant to 47 C.F.R § 64.2009(e), for The Hamilton Telephone Company (ID: 801915) and Hamilton Long Distance Company (ID: 801916).

Sincerely,

A handwritten signature in blue ink, appearing to read "John Nelson", with a long horizontal flourish extending to the right.

John Nelson  
Vice President  
Hamilton Telephone Company  
Hamilton Long Distance Company

Attachments:  
CPNI Certification  
Operating Procedures for Compliance with CPNI Rules

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

## EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: 02/19/2018
2. Name of company(s) covered by this certification:  
The Hamilton Telephone Company; Hamilton Long Distance
3. Form 499 Filer ID: 801915; 801916
4. Name of signatory: John Nelson
5. Title of signatory: Vice President
6. Certification:

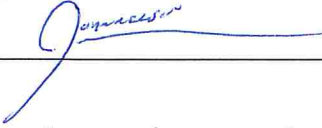
I, John Nelson, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (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 company has 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 company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges 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  [Signature of an officer, as agent of the carrier]

**Attachments:** Accompanying Statement explaining CPNI procedures

Updated 2015

Operating Procedures for Compliance with CPNI Rules  
Hamilton Telephone Company (ID: 801915)  
Hamilton Long Distance Company (ID: 801916)

Hamilton Telephone Company and Hamilton Long Distance Company (hereinafter "Hamilton") have implemented the following procedures to ensure compliance with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Network Information (CPNI), 64.2001 through 64.2011. The purpose of these procedures is to safeguard customer information.

**Compliance Officer**

Hamilton has appointed a CPNI Compliance Officer and a back-up Compliance Officer. The Compliance Officer is responsible for ensuring that Hamilton 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. The back-up Compliance Officer will follow all Operating Procedures in the absence of the Compliance Officer.

**Employee Training**

CPNI regulatory training is required for marketing personnel and Hamilton's personnel who interact with customers and customer accounts. Employees are trained on an annual basis and more frequently if needed. Newly hired employees are assessed to determine if CPNI training is applicable. If so they will receive the proper training as required by Hamilton's policy. The training includes, but is not limited to, when employees are and are not authorized to use CPNI, and on the authentication methods that Hamilton is using. The detail of the training can differ based on whether or not the employee has access to CPNI.

After completing this training, all employees for whom this training is required are also required to sign a certification that they have received training on the CPNI rules, that they understand Hamilton's procedures for protecting CPNI and they understand Hamilton's disciplinary process for improper use of CPNI. A CPNI manual that includes the rules is available at each employee's location.

All employees exposed to CPNI have been instructed that if they have any questions regarding the proper use of CPNI, or if they are aware of CPNI being used improperly by anyone, they should contact the Compliance Officer immediately.

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

Hamilton has provided notification to its customers of their CPNI rights and has asked for the customer's 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 so that employees can readily identify customers that have restricted the use of their CPNI.

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

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

Hamilton does not share CPNI with any joint venture partner, independent contractor or any third party.

Hamilton will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

A copy of the most recent notification is kept in the CPNI official files.

## **Marketing Campaigns**

Hamilton does not do any outbound marketing campaigns. But, if in the future we do outbound marketing, we must establish a supervisory review process for the marketing campaign and it must be approved by the Compliance Officer.

## **Customer Authentication Process**

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

**In-office visit** – the customer, or an individual that has been authorized by the customer to access the account, must provide a valid photo ID.

**Telephone inquiry** – the customer, or an individual that has been authorized by the customer to access the account, is authenticated by providing the established answer to our question for that specific account. If a customer calls and the answer to our authentication question has not been established, a Hamilton employee will contact the customer. The employee will do this by calling the customer's telephone number of record, mailing the customer at their address of record or ask the customer to come into the office with a valid photo ID to establish the answer to our authentication question.

Hamilton has not established a "password" for providing call-detail to its customers. A request for call-detail is handled as follows:

- If the customer can provide all of the call detail information (telephone number called, when it was called, the amount of the call, etc.) necessary to address the customer's issue, Hamilton 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, Hamilton will: (1) call the customer back at the telephone number of record, (2) send the information to the address of record, or (3) ask the customer to come into the office and provide a valid photo ID.

## **Customer Notification of Account Changes**

Hamilton notifies customers of any changes that have been made to their account, either by sending a notification to the address of record or by calling the telephone number of record. If the customer did not authorize any change, they are asked to contact our office immediately.

## **Disciplinary Process**

Hamilton has established a specific disciplinary process for improper use of CPNI. The disciplinary action is based on the type and severity of the violation. All violations will include retraining the employee on the CPNI rules. Additional disciplinary action could include any or all of the following: making a notation in the employee's personnel file, a formal written reprimand, suspension or termination.

A single incidence of an unintentional violation could be cause for the least severe discipline while intentional and/or multiple violations could be cause for the most severe discipline.

The disciplinary process is included in the employee handbook under CPNI regulations. It has been reviewed with each employee that works with CPNI.

## **Notification of Breaches**

A breach occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI with an intent to cause harm.

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:

1. Notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) as soon as possible, but not later than 7 business days after determination of the breach via their electronic link at <http://www.fcc.gov/eb/cpni>.

2. Notify the customer only after 7 business days have passed since notification to the USSS and FBI, unless the USSS or FBI has requested an extension.
3. Maintain a record of the breach, the notifications made to the USSS and FBI and the notifications made to the customer. A detailed description of CPNI that was the subject of the breach, dates they occurred, how the breach occurred, impact of the breach, proof of notification to law enforcement and other pertinent details will need to be kept.
4. All records will be maintained for 2 years and explained in the annual certification.

### **Miscellaneous**

Hamilton's CPNI policies include reasonable measures to discover and protect against activity that is indicative of pretexting as well as any other unauthorized attempts to access CPNI. Employees are instructed to notify the CPNI Compliance Officer of any suspicious activity. The Compliance Officer will determine what action needs to be taken.

### **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.