Algona Municipal Utilities

104 West Call St., P.O. Box 10
Algona, Iowa 50511-0010
Email: amu@netamu.com

Telephone (515) 295-3584
Fax (515) 295-3364
Web: www.netamu.com

February 13-2009

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, D.C. 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 Algona Municipal Utilities.

Sincerely,

John Bilsten
General Manager

Attachment

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

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008.

Date filed: 2-13-2009

Name of company(s) covered by this certification: Algona Municipal Utilities

Form 499 Filer ID: 822832

Name of signatory: John Bilsten

Title of signatory: General Manager

I, John Bilsten, 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.

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

Signed _____

OPERATING PROCEDURES FOR COMPLIANCE WITH CPNI RULES

Algona Municipal Utilities (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. Employees are informed as to where the Company's CPNI manual with rules is located in the office.

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 FCC states that the company must have an express disciplinary process in place for improper use of CPNI by employees. The disciplinary guidelines must apply to both a "breach" and the accidental misuse by an employee.

The Company's disciplinary process is outlined in this section and is also included in the personnel manual for the Company.

The FCC does not state what action needs to be taken against an employee so the Company has established the following policy.

1. An employee accidentally used CPNI without first getting a customer's approval.

    a. For the first and second violation, the CPNI rules will be reviewed with the employee again and documentation will be placed in the employees personnel file. The employee will also be made aware that a third violation may mean termination from employment depending on the circumstances of the accidental use of CPNI data without first getting customer approval.

2. An employee used CPNI to intentionally do harm to a customer or to obtain self-profit from use of CPNI.

    a. This type of activity will not be allowed by the Company. Any employee who uses CPNI in this matter will be immediately terminated from employment at the Company.

3. A data broker obtains CPNI because of an employee's negligence.

    a. This is a very serious violation, even though it may not have been intentional. The Company will suspend the employee without pay for three days and the CPNI rules will be reviewed with the employee again and documentation will be placed in the employees personnel file.

The disciplinary process is reviewed with all employees.

A copy of the Company's disciplinary process is kept in the Algona Municipal Utilities Personnel Manual and in the CPNI manual.

Customer Notification and Request for Approval to Use CPNI

The Company has provided notification to its customers and has asked for approval to use CPNI in those instances where it is permissible to use CPNI without customer approval. It does not share the customer's CPNI with any joint venture partner, independent contractor or any other third party. 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.

A copy of the customers CPNI information is kept in the customers file. The most recent CPNI notification is kept in the CPNI official files.

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 or answers correctly all the authentication questions previously established.

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 or be the account holder.

If the customer wants to discuss call detail information that requires a password after establishing authentication, 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: (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.

Notification of Account Changes

The Company promptly notifies customers whenever a change is made to any of the following:

- Customer response to a back-up means of authentication for a password.
- Online account.
- Address of record.

The notification to the customer will be made either by a Company-originated voicemail or text message to the telephone number of record or sent to the address (postal or electronic) 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 billing software provides a notification to the Company when an account change takes place. The billing software also allows the Company to track a date that a letter was sent to a customer.

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.

- 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 in a CPNI manual located in the Company office with its location indicated to all Company employees who are covered under the CPNI rules. Following is the minimum retention period we have established for specific items:

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