

EB Docket 06-36
Customer Proprietary Network Information (CPNI)

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009.

Date filed: March 1, 2010.

Name of companies covered: Matanuska Telephone Association, Inc. and its subsidiary, MTA Communications, Inc.

Form 499 Filer ID: 804969 & 809610

Name of signatory: Donald J. Reed

Title of Signatory: Director of Regulatory Affairs and Carrier Relations

Certification:

I, Donald J. Reed, 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, 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



Donald J. Reed, Director of Regulatory Affairs and Carrier Relations

Attachment: Accompanying Statement explaining CPNI procedures.

“Accompanying Statement Explaining CPNI Procedures”

Customer Proprietary Network Information

CPNI is defined by the Telecommunications Act as the information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, that is made available to the carrier by the customer solely by virtue of the customer-carrier relationship, and is contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. CPNI does not include subscriber list information.

MTA Customer Privacy

Matanuska Telephone Association, the local exchange carrier, and its affiliate MTA Communications respect and protect member/subscribers' privacy and comply with the Telecommunications Act and associated FCC regulations governing the use of customer proprietary network information (CPNI). Customer service personnel are trained to keep all customer records confidential. The MTA Customer Service department is committed to the compliance of CPNI requirements. To ensure that all Sales and Customer Service personnel are following CPNI requirements, two written Standard Operating Procedures (SOP) have been implemented: Customer Proprietary Network Information (CPNI), SOP – 544, Revision 3; and CPNI – Customer Verification Code SOP – 545, Revision 5. These procedures are written by the Customer Care Process Analyst who works with several departments and supervisors to develop and update these standards. In addition, the Analyst attends staff meetings of all Sales and Customer Service offices on a regular basis to disseminate and promote the understanding of these procedures. Updates to CPNI procedures are provided at staff meetings.

New employees are oriented on CPNI policy and procedures by attending a training session with their supervisor. Details of SOP – 544 and SOP – 545 are reviewed during the training session. Topics that are covered include: purpose, procedures, setting up/changing a verification code, scripting, customer forgetting verification code, setting up a security question and answer, former MTA customers, and when a verification code is not required. Common customer scenarios are discussed in this training. New representatives are paired with experienced representatives who work closely with them. Customers are notified that calls to Sales and Customer Service are electronically recorded to ensure quality assurance. Supervisors listen to these calls randomly to ensure adherence to CPNI standards. Any questions regarding information that can be released are referred to supervisors. The supervisors follow strict policy regarding the release of information.

All employees at MTA read and acknowledge receipt of MTA's Secrecy of Communications policy at the time of hire. The failure of an employee to observe and follow this company policy is subject to discipline, up to and including dismissal. To add an additional layer of security, MTA now requires all employees who have access to CPNI to read and acknowledge receipt of MTA's CPNI policy. MTA work rules expressly forbid the disclosure of confidential information to anyone unless directed to do so by a supervisor.

MTA further protects the security of its customer's privacy through its electronic network policies. A supervisor's approval is required before an employee has access to any electronic database of MTA's records. Further, MTA takes all reasonable efforts to maintain the security of its electronic network from invasion by unauthorized users.

MTA has implemented the password requirement for CPNI requests into our daily interactions with customers. To further protect customer information which is not considered CPNI, MTA has enacted a

company policy that all customers who call in to discuss their account be required to authenticate themselves using the CPNI authentication methods required by the FCC.

The new FCC requirements require CPNI information to only be released after a customer has authenticated themselves. MTA has procedures in place for use when a customer is unable to authenticate themselves by password or backup question. If a customer calls in and forgets their password and is unable to answer a backup question, the customer service representative is required to either call the customer back at their number of record, inform the customer that the information will be mailed to their address of record, or request the customer come in to the office and present photo identification. These alternative authentication methods ensure that customer data remains safe from unauthorized individuals.

If a customer chooses to change information on their account or alter their services, a program within the database has been created which automatically flags that person's information and a label is generated which is then attached to a mailer and sent out to the customer address of record prior to any changes. The mailer informs the customer a change has been made to their account and a phone number is provided for them to call if they have any questions.

New customers to MTA are informed about CPNI and why they need to protect their information. Customers are asked to provide a CPNI password and backup authentication answers at the time the customer initiates service with the company. After the customer has been in service for 30 days, a mailer is sent out detailing our CPNI policy and how CPNI is used internally. After 60 days a second letter is mailed informing the customer of our opt-out policy. The mailer informs the customer they have the right to request their information not be used for marketing purposes.

MTA has instituted a breach notification policy which covers internet and traditional breaches. Both are taken seriously and handled expeditiously. All customer service representatives have been trained to understand the breach policy and what steps must be followed to report that breach. For a traditional breach, the representative is required to fill out a CPNI Breach Notification Form. This form contains the customer's information, the representative's information who handles the complaint, and finally a narrative of the complaint being reported. This form is then submitted to both the representative's immediate supervisor as well as the Regulatory Affairs Department. All complaints must be submitted within 48 hours of notification internally. Regulatory Affairs then takes this information and reports the breach via the breach reporting portal, <https://www.cpnireporting.gov/dtrp/content/disclaimer.faces>). As required by the FCC, these complaints are processed within 7 days of the initial complaint. MTA will not notify the customer of the resolution to their complaint until law enforcement has investigated the breach and given permission to proceed with notification.

A breach of the customer database or a customer's online portal is handled by our IT department. Their response to the breach is immediate. An incident commander is assigned who will be the main contact person for details pertaining to the breach. A severity level will be assigned with 1 being a major incident and 3 being a minor incident. During the processing of the breach, hourly reports are given to the IT managers, as well as the Executive Manager of the IT department. Once the breach has been contained, a formal report is then written and sent to management and Regulatory Affairs for processing. An online breach is handled in a similar fashion as the traditional breach in that the breach is submitted to law enforcement via the breach portal within 7 days of the incident.

Marketing Campaigns

MTA has implemented an opt-out policy for CPNI. Customers are given the opportunity annually to opt-out of any marketing campaigns that take place during the year. Each customer receives two notices each year. The first notice sent to customers is a flyer which educates them on CPNI and its possible uses. The second notice sent 30 days later is a letter which informs the customer that MTA has adopted an opt-out policy. The customer is asked to do nothing if they want to be part of marketing campaigns. If the customer chooses to opt-out, we give them the option of calling us, emailing us, or notifying us by regular mail. Customers are asked to respond within 30 days if they choose to opt-out. If at any time a customer who has opted in changes their mind, they can choose to opt-out at any time during the year by using the same methods discussed above.

To ensure proper accounting of CPNI status, all customer data maintained in the database is assigned a specific indicator as to CPNI status. All customers who notify us that they are opting out are assigned a flag within the system alerting Marketing and Customer Service that this customer wishes to be excluded from any marketing campaigns. Those who have chosen to opt-in have a comment in the CPNI field indicating that the customer wishes to participate in advertising campaigns. The CPNI field within the database can only be changed by a service order. When a marketing campaign is being planned, a query is run on the customer database and all customers who have the opt-out flag assigned to them are purged from the list. The final customer list contains those who have opted in. All marketing campaigns are tracked by a database which contains the campaign name, date it was kicked off, and how CPNI information was used for that campaign. The database is maintained within our marketing department and is purged annually.

Complaints and Filings Regarding CPNI

During the calendar year beginning January 1, 2009 and ending December 31, 2009, MTA and its affiliate MTA Communications received zero complaints in regards to CPNI usage or breaches. During this same calendar year no reports or proceedings were initiated by either company against data brokers to the FCC or the Regulatory Commission of Alaska. MTA is aware that pretexters and their ability to obtain data are a major threat to customers and MTA has instituted all requirements by the FCC into the daily operations of the company as well as implementing procedures for protecting non-customer detail information. By instituting the different procedures explained in this statement, MTA believes it is doing everything in its power to protect its customers and their data.