

MONTEZUMA
TELEPHONE AND CABLE COMPANY
a subsidiary of Iowa Telecom

PO Box 10
Montezuma, Iowa 50171

Office: 641.623.5654
Fax: 641.623.2199

February 25, 2010

Marlene H. Dortch, Secretary
Office of the Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

RE: EB Docket 06-36
Annual Certification and Accompanying Statement for 2009
499 Filer ID: 801606

Dear Ms. Dortch:

Montezuma Mutual Telephone Company ("Montezuma") submits the Annual Certification and Accompanying Statement for 2009 for the incumbent local exchange operations as required by 47 C.F.R. § 64.2009(e) and in accordance with the Public Notice DA 10.91, issued on January 15, 2010. A copy of the Annual Certification and Accompanying Statement for 2009 for Iowa Wireless Services d/b/a i wireless is also attached. The underlying provider for Montezuma wireless service is i wireless.

If you have any questions or need additional information, please contact me directly on 641-787-2396.

Sincerely,



Barbara E. Bouley
Manager-Regulatory

Cc: Best Copy and Printing, Inc (1 copy)
Via e-mail FCC@BCPIWEB.COM
445 12th Street
Suite CY-B402
Washington, DC 20554

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: February 25, 2010

Name of company covered by this certification: Montezuma Mutual Telephone Company

Form 499 Filer ID: 801606

Name of signatory: Dennis R. Kilburg

Title of signatory: Vice President

I, Dennis R. Kilburg, 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 did not take any actions against data brokers in 2009.

The company did not receive any customer complaints in 2009 concerning the unauthorized release of CPNI.

Signed


Dennis R. Kilburg

Montezuma Mutual Telephone Company

Compliance Statement

Montezuma Mutual Telephone Company (“Montezuma”) has the following safeguards in place to ensure compliance with Section 222 of the Communications Act of 1934, as amended.

- Personnel (both sales and marketing) receive training as to when they are and are not authorized to use customer proprietary network information (“CPNI”), and an express disciplinary procedure is in place when a Montezuma policy is not followed. Training is included as part of the initial training and refresher training as required.
 - CPNI may be used, disclosed or access permitted for the purpose of marketing service offerings among the category of services to which the customer already subscribes.
 - Where the company and/or its affiliates provide different categories of service and the customer subscribes to more than one category of service, CPNI may be shared among the affiliated entities that provide a service to the customer.
 - Where the company and/or its affiliates provide different categories of service and the customer does not subscribe to more than one offering, CPNI may not be shared among the affiliated entities that provide a service to the customer unless the customer provides permission to share the information.
- Montezuma provides all new customers with an explanation of CPNI and a form to submit to the company if they choose to opt-out of the use of their CPNI. Once a customer notifies the company that they choose to opt-out, the use of the CPNI is restricted until such time as the customer notifies the company to change the opt-out status of their account.
- The customer may dial 1-641-623-5654 or email info@zumatel.net to request opting-out of the use of the CPNI on their account.
- Biennial notification that includes an explanation of CPNI and how the customer may request opting-out of the use of the CPNI on their account is sent to all customers.
- The customer’s CPNI approval status is clearly visible on the account records.
- CPNI is not provided to or disclosed to third parties. Montezuma does not disclose or provide access to joint venture partners or independent contractors.
- Records are retained at least one year of the sales and marketing campaigns using CPNI. The records include a description of each such campaign, the dates and

purpose of the campaign, the specific CPNI used, and the products and services offered.

- Supervisory approval is required to develop out-bound marketing plans for mailings and calling campaigns.
- Montezuma has systems in place to establish and maintain password protection on the customer's account and to allow the customer to establish a security question and answer in the event the password is forgotten or lost.
- Montezuma properly authenticates the customer prior to releasing call-detail information without using readily available biographical information or account information. Where the customer cannot provide the password but can provide call detail information to Montezuma without assistance, Montezuma will respond to the specific question. Where the customer cannot provide the password or call detail information, Montezuma will send the call detail information to the customer's address of record or call the customer at the telephone number of record.
- In-store access to CPNI is allowed only upon presentation of a valid photo ID matching the customer's account information.
- On-line access to account information is not currently available.
- Montezuma notifies customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, or address of record are changed.
- The requirements under 47 C.F.R. § 64.2011 *Notification of customer proprietary network information security breaches* will be followed should a breach of its customers' CPNI occur.

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: Feb. 16, 2010

Name of company covered by this certification: Iowa Wireless Services, LLC d/b/a i wireless

Form 499 Filer ID: 819238

Name of signatory: David Frost

Title of signatory: Chief Financial Officer

I, David Frost, certify that I am an officer of Iowa Wireless Services, LLC d/b/a **i wireless**, and acting as an agent of the company, that I have personal knowledge that **i wireless** 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 is **i wireless's** CPNI Policy and Procedures manual. The policy and procedures manual explains how **i wireless'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. All employees receive instruction in the company's CPNI policies and are required to sign a receipt and acknowledgment statement annually.

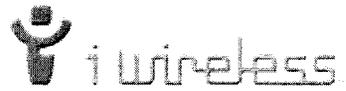
i wireless does not sell or release CPNI to third parties for marketing purposes. **i wireless** maintains the required records of its marketing campaigns soliciting current or previous customers for services or products. **i wireless** maintains records of customers that have asked not to receive solicitations and does not contact those customers in marketing campaigns. **i wireless** has a supervisory review in place that requires all marketing and sales campaigns to be approved by a supervisor.

i wireless has not taken any actions (proceedings instituted or petitions filed at either state commissions, the court system, or at the Commission) against data brokers in the past year. **i wireless** is not aware of any attempts of unauthorized access to CPNI by pretexters. The steps taken to protect CPNI are outlined in the attached CPNI Policy and Procedures manual.

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

Signed: David Frost

David Frost
Chief Financial Officer
Iowa Wireless Services, LLC d/b/a i wireless



IOWA WIRELESS SERVICES, LLC

**POLICY AND PROCEDURES
GOVERNING
CUSTOMER PROPRIETARY NETWORK INFORMATION**

Iowa Wireless Services, LLC
4135 N.W. Urbandale Drive
Urbandale, IA 50322

Table of Contents

Table of Contents.....	i
Introduction & Statement of Company Policy	1
1.0 Applicability	2
2.0 Definitions	2
3.0 General Duty of the Company	3
4.0 Confidentiality of Carrier Information	3
5.0 Confidentiality of CPNI.....	3
6.0 Conduct Expressly Prohibited By the Company	3
7.0 Permitted Uses and Disclosures of CPNI	4
8.0 Company Policies & Procedures	5
Receipt and Acknowledgment.....	9

Introduction & Statement of Company Policy

Under applicable federal and state laws, Iowa Wireless Services (the “Company”) has a duty to protect the confidentiality of proprietary information of, and relating to, customers, other telecommunication carriers, and equipment manufacturers. To ensure full compliance with these laws and regulations, including, specifically, the rules of the Federal Communications Commission governing customer proprietary network information (“CPNI”), this Manual sets forth in detail the policy and procedures of Iowa Wireless Services governing the use, disclosure, and provision of access to such proprietary information.

Questions regarding compliance with the policies and procedures set forth in this Manual should be directed to the Company’s Chief Financial Officer.

STATEMENT OF COMPANY POLICY

Each employee and authorized agent of the Company is required to protect the confidentiality of **customer proprietary network information** (“CPNI”) and, to that end, shall comply with all policies and procedures set forth in this Manual.



Each employee and authorized agent of the Company is required to protect the confidentiality of proprietary information of other **telecommunications carriers** and **equipment manufacturers**, and to that end, shall comply with all policies and procedures set forth in this Manual.



Any violation of or departure from the policies and procedures set forth in this Manual shall be reported to the Company’s Chief Financial Officer.



Any failure to comply with the policies and procedures set forth in this Manual shall result in disciplinary action including, but not limited to, suspension and/or termination of employment.

1.0 APPLICABILITY

The policies and procedures set forth in this Manual apply to all employees, officers, directors, and authorized agents of Iowa Wireless Services, LLC (or the "Company").

2.0 DEFINITIONS

- 2.1 "Customer proprietary network information" means --
- (a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
 - (b) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.
- 2.2 *Account information.* "Account information" is information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.
- 2.3 *Address of record.* An "address of record" whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.
- 2.4 *Call detail information.* Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.
- 2.5 *Readily available biographical information.* "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.
- 2.6 *Telephone number of record.* The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."
- 2.7 *Valid photo ID.* A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

3.0 GENERAL DUTY OF THE COMPANY (47 U.S.C. § 222(a))

The Company, including all employees, officers, directors, and authorized agents of the Company, have a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

4.0 CONFIDENTIALITY OF CARRIER INFORMATION (47 U.S.C. § 222(b))

The Company may use proprietary information received or obtained from another telecommunications carriers for the purpose of providing any telecommunications service only for that purpose. The Company may not use such information for its own marketing efforts.

5.0 CONFIDENTIALITY OF CPNI (47 U.S.C. § 222(c))

5.1 Privacy Requirements - Generally. The Company may only use, disclose, or permit access to individually identifiable CPNI –

- (a) as **required by law**;
- (b) with the **approval of the customer**; or
- (c) **in providing the telecommunication service from which the CPNI is derived** or in providing services necessary to, or used in, providing such telecommunications service.

5.2 Disclosure upon Request by Customers. The Company shall disclose CPNI, upon affirmative written request by the customer, to any person designated by the customer.

6.0 CONDUCT EXPRESSLY PROHIBITED BY THE COMPANY

6.1 The following are expressly prohibited by the Company:

- (a) Sale or possession of CPNI.

The Company prohibits the sale and/or possession of CPNI, and any other conduct undertaken for a fee for the purpose of using, disclosing, or permitting access to CPNI in violation of § 5.1 of this Manual. The Company prohibits any attempt to sell, obtain possession of, or otherwise

acquire or arrange for unauthorized access to CPNI, including any effort to induce another to permit an unauthorized use, disclosure or access to CPNI.

(c) Use of CPNI to track customers' use of competitors' services.

The Company prohibits the use, disclosure or provision of access to CPNI to identify or track customers that call competing service providers.

- 6.2 Any violation of this section shall be grounds for immediate termination of employment and, as applicable, referral to federal and/or state law enforcement authorities for further action. The Company may, however, in its discretion take alternative disciplinary action against any employee, officer, director or authorized agent of the Company found to have violated this section.

7.0 PERMITTED USES AND DISCLOSURES OF CPNI

The Company may use CPNI obtained from its customers, either directly or indirectly through its agents --

- 7.1 To initiate, render, bill and collect for telecommunications services;
- 7.2 To provide marketing, in compliance with FCC 64.2005(a);
- 7.3 To protect the rights or property of the Company, or to protect users and other carriers from fraudulent or illegal use of, or subscription to, such services;
- 7.4 To provide call location information concerning the user of a commercial mobile service in the following emergency situations:
- (a) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;
 - (b) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or
 - (c) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency;
- 7.5 For the provision of information services;
- 7.6 In its provision of maintenance and repair services.

8.0 COMPANY POLICIES & PROCEDURES

8.1 Unauthorized Use of CPNI.

The Company regards any unauthorized or improper use, disclosure or access to CPNI as a serious offense, and will take appropriate disciplinary action, which may include suspension and/or termination of employment. In addition:

- (a) The Company may require any employee, officer or director found to have made unauthorized or improper use of CPNI to undergo training to ensure future compliance.

8.2 CPNI Requested by Law.

An employee who receives a request to provide CPNI pursuant to legal process, such as a subpoena or warrant, shall provide such information only after verification of the identity of the requesting agency or officer.

8.3 Customer Requests for CPNI.

- (a) CPNI may be disclosed only to the customer or a third party designated by the customer to receive the customer's CPNI. The Company requires all employees to ensure that the person requesting CPNI is authorized to receive such CPNI. The company requires authentication of a customer's identification prior to the release of CPNI on customer initiated telephone contacts, online account access, or in-store visit.
- (b) The Company does not accept customer requests for CPNI via facsimile or email.
- (c) The Company will disclose call detail on a customer initiated call only if the customer provides a pre-established password to confirm the customer's identity. If no password has been established or if the customer does not provide a password the company will not release the information except by sending them to an address of record or by calling the customer at the telephone of record. If the company calls the customer at the telephone of record, the customer must provide identity authentication. Identity authentication may include his or her full name, street address, social security number, and date of birth.. If identity authentication cannot be confirmed, the customer must make his or her CPNI request in person at the Company's office or one of its retail facilities and produce a government-issued personal identification with a photograph such as a current driver's license, passport, or comparable ID matching the customer's account information before CPNI will be provided.

- (d) If the customer is able to provide call detail information to the Company's employee during a customer-initiated call without the Company employee's assistance, then the employee is permitted to discuss the call detail information provided by the customer.
- (e) The Company will disclose non-call detail CPNI on a customer initiated call if the customer provides identity authentication. Identity authentication may include his or her full name, street address, social security number, and date of birth.
- (f) The Company allows CPNI to be disclosed to a third party designated by the customer to receive his or her CPNI only pursuant to written authorization from the customer. The following is required for a written authorization to be valid: the customer's full name, street address, social security number, date of birth, and the telephone number(s) for which CPNI is requested. The authorization must be signed by the person whose name appears on the account as the customer of record. The Company will accept only a signed original authorization.

8.4 Online account Access.

The Company requires a password or back-up authentication to access CPNI on line. Back-up authentication may not include readily available biographical information. If a customer cannot provide a password or the proper response to back-up authentication, the company will authenticate the customer based upon the methods listed in 8.3 (c).

8.5 Notice to Customers of Account Change.

The Company will notify the customer immediately when the following are created or changed: (1) a password; (2) a back-up for forgotten passwords; (3) an online account; (4) the address of record. This notification may be through a Company originated voicemail or text message to the telephone number of record, or by mail to the address of record, as to reasonably ensure that the customer receives the notification.

8.6 Records of Disclosure of CPNI.

The Company shall maintain a record of its own or any affiliates sales and marketing campaigns (if any) that use their customers' CPNI. The Company's Vice President of Sales & Marketing is responsible for maintaining this record, which shall include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. This record shall be kept for a minimum of one year.

8.7 Duty to Report Violation or Departure from CPNI Policies and Procedures Manual

Each employee, officer, director and authorized agent of the Company has an affirmative duty to ensure compliance by the Company of the requirements under federal and state law governing the use of CPNI. Any employee, officer, director or authorized agent of the Company who knows of or has reason to believe that a violation of or departure from the policies and procedures set forth in this Manual has occurred or will occur shall immediately notify your immediate Manager/Supervisor, Executive Officers, the CEO, or any member of the Board of Directors if the CEO is the subject of the suspected violation.

8.8 Notice to Law Enforcement of Unauthorized Disclosure of CPNI

- (a) The Company must notify law enforcement of a breach of its customer's CPNI no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the Federal Bureau of Investigation . The Company will not notify customers or disclose the breach to the public until 7 full business days have passed after the notification to the USSS and the FBI except as provided in FCC § 64.2011 (b) (2) (3).
- (b) The company will maintain a record of any breaches discovered, notifications made to the USSS and the FBI and notifications made to customers. The record will include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach and the circumstances of the breach. The record must be retained for 2 years.

8.9 Employee Annual Certification

All employees of the Company shall be given a copy of this Manual. All employees are required annually to review the manual and to certify in writing that he or she understands and will adhere to the policies and procedures in this manual.

8.10 Annual Certificate of Compliance.

A Company Officer shall annually sign a CPNI compliance certificate stating that the officer has personal knowledge that the Company has established policies and procedures that are adequate to ensure compliance with the FCC's CPNI rules.

RECEIPT AND ACKNOWLEDGMENT

I acknowledge that I have received a copy of the manual on Iowa Wireless's Policies and Procedures Governing Customer Proprietary Network Information ("Manual"). I understand that I am responsible for knowing and adhering to the policies within the Manual. I understand that any infractions of the forgoing policies may constitute grounds for the termination of my status with the company, or other disciplinary measures.

Signature _____

Print Name _____

Company Iowa Wireless Services, LLC d/b/a
i wireless

Location _____

Date _____