417 Wayne Avenue, Suite 102
Defiance, OH 43512
(419) 782-6990

February 22, 2017

Via Electronic Filing

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

RE: EB Docket No. 06-36
Annual CPNI Certification –QualStar Communications, Inc.

Dear Secretary Dortch:

Enclosed for electronic filing is QualStar Communications, Inc.'s annual 64.2009(e) CPNI Certification for 2017 covering calendar year 2016. Please contact me at 419-782-6990 or via email at todd.harpest@qualstar.net if you have any questions regarding QualStar's certification.

Thank you.

Very truly yours,

Todd Robert Harpest

Todd Harpest
Manager

cc: via email – FCC@BCPIWEB.com

Enclosure

BEFORE
THE FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

EB-06-TC-060

EB Docket No. 06-36

ANNUAL 47 C.F.R § 64.2009(e) CPNI CERTIFICATION

Annual 64.2009(e) CPNI Certification for 2017 covering the prior calendar year 2016

Date filed: February 22, 2017

Name of company covered by this certification: QualStar Communications, Inc.

Form 499 Filer ID: 801288

Name of signatory: Todd Harpest

Title of signatory: CPNI Compliance Officer

I, Todd Harpest, certify that I am the CPNI Compliance 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 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 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 10 of the U.S. Code and may subject it to enforcement action.

Signed Todd Robert Harpest

Attachments: Accompanying Statement explaining CPNI procedures

QUALSTAR COMMUNICATIONS, INC.
STATEMENT OF CPNI PROCEDURES

QualStar Communications, Inc. has created a CPNI Policy Handbook containing the following procedures that it has adopted to ensure the protection of CPNI. The handbook describes our procedures in greater detail and provides practical guidance on how to protect against unauthorized disclosure or use of CPNI. The handbook is distributed to our employees during training and serves as an important reference tool for our employees.

Duty to Protect CPNI

We as a communications company recognize our duty to protect customer CPNI. We may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

1. Administrative use: We may use CPNI to *initiate, render, bill and collect* for communications services.

2. Protection of carrier and third parties: We may use CPNI to protect the interests of our company, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.

3. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

Our Own Use Of CPNI

We may use CPNI to provide or market services to our existing customers. We understand that we are required to obtain customer approval prior to using CPNI in certain ways.

Marketing

We understand that we do not need to obtain customer approval before using CPNI to market services to our existing customers within the categories of service to which the customer already subscribes.

We understand that we may not use CPNI to market services that are in a service category to which the customer does not already subscribe without customer approval.

We understand that we cannot use CPNI to solicit a customer to add a new category of service without first obtaining the customer's approval.

We also understand that we do not need customer consent before using CPNI to market "adjunct-to-basic" services such as speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain centrex features.

We understand that we may not use CPNI to identify or track customers that call competing service providers.

We regularly review our marketing practices to determine when and how CPNI is used within the company, and whether CPNI is being shared with other entities. We also review new marketing or sales campaigns to ensure compliance with these CPNI policies and with the FCC's CPNI regulations. We do not share CPNI with our affiliates or other third parties.

Provision of Services

We understand that we do not need customer approval to use CPNI to provide CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

Authenticating Customers Before Disclosing CPNI

We understand that we are required to objectively determine that our customers are who they say they are before disclosing CPNI to them.

Telephone

We understand that when a customer calls, we may not release *call detail information*, or information relating to the transmission of specific telephone calls until we have obtained the account password from the caller, or called the customer back at the telephone number of record to ensure that the customer is who s/he says s/he is. Alternatively, we may offer to send the call detail information to the address of record or provide it to the customer or an authorized individual in person after s/he has produced valid photo identification at our office.

We understand that we may disclose *non-call detail information* over the telephone after authenticating the customer by calling back the telephone number of record, checking valid photo identification, or by mailing the information to the account address of record.

In-Person Authentication

We understand that before we can disclose CPNI to customers in person, the customer must present *valid government-issued photo identification*. The name on the photo identification must match the name on the account. If the customer cannot present the required identification, we offer to provide the requested CPNI by sending it to the account address of record.

Before providing the CPNI to the customer, we make a copy of the photo identification. This copy is then placed in the customer's file, together with a copy of the CPNI provided to the customer. These records are then kept in the customer file in accordance with our record-keeping policies.

Mail

If the customer requests CPNI through regular mail, or if the customer cannot comply with one of the authentication methods above, we send the requested information to the customer's address of record only.

Customer Notification of CPNI Rights

We provide a CPNI privacy policy to all customers annually, via mail during the first quarter. This policy provides notification to each customer of his/her right to restrict use of, disclosure of, and access to that customer's CPNI. We maintain a list of all customers who receive the privacy policy, the date on which the policy is sent, and a copy of the policy in our records for two (2) years following the mailing of the policy. We provide additional copies of the CPNI privacy policy to all customers who request it and to all new customers upon activation of service.

The policy contains an opt-out customer approval notice. Customers who do not wish to allow us to use their CPNI to market services outside their existing service categories, or who do not wish to allow us to share their CPNI with affiliates, have 30 days to contact us to tell us that they do not approve of this use. If we do not hear back from the customer within 30 days, we understand that we are free to use their CPNI for these purposes. We understand that customers can change their option at any time by contacting us, and we notify our customers of this right.

We maintain records of the customers who received the opt-out approval notice and records of the customers who contacted us to opt out in accordance with our record-keeping policies.

We understand that we must provide written notice to the FCC within five (5) business days if our opt-out mechanisms do not work properly to the degree that our customers' inability to opt out is more than an anomaly.

Training And Discipline

We trained our Customer Service Representatives, Accountants, and Management Team regarding the company's CPNI policies prior to the effective date of the most recent CPNI regulations. We also trained our technicians regarding the company's CPNI policies shortly after this effective date to ensure that all employees with access to confidential customer information have the proper training regarding protection of CPNI. Employees are required to attend an annual training in the fourth quarter of the prior year to ensure that they understand the company's CPNI policies and any updates to those policies. New employees who will have access to CPNI are trained when they join the company, and then attend the regularly-scheduled retraining sessions. At the conclusion of each training session, employees are asked to sign certificates stating that they understand the company's CPNI policies and that they will comply with those policies.

We have implemented the following disciplinary guidelines for employees who fail to follow our CPNI policies:

> Employees who fail to observe QualStar Communications, Inc's CPNI policies will be subject to the following discipline: verbal warning, written warning, separation. Records relating to this process will be maintained in the company files in line with the record-keeping policies outlined below.

Disciplinary records are maintained in the company files in accordance with our record-keeping policies.

Record-Keeping

We maintain the following records in our files for two (2) years:

a. Records relating to the annual mailing of the customer CPNI privacy policy;

b. Records of customer approval or disapproval of CPNI use, or the limitation or revocation thereof;

c. Employee disciplinary records; and

d. Records of discovered CPNI breaches, notifications to law enforcement regarding breaches, and any responses from law enforcement regarding those breaches.

Notification Of Account Changes

We understand that we are required to notify customers when changes have been made to passwords, customer responses to back-up means of authentication, or addresses of record by mailing a notification to the account address of record.

We do not reveal the changed account data in the notification.

Unauthorized Disclosure Of CPNI

We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at http://www.fcc.gov/eb/CPNI/ to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

Records relating to such notifications are kept in accordance with our record-keeping policies. These records include: (i) the date we discovered the breach, (ii) the date we notified law enforcement, (iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

Signed _____