CROCKER & CROCKER
ATTORNEYS AT LAW

PATRICK D. CROCKER
patrick@crockerlawfirm.com

February 18, 2019

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

Filed Electronically Via ECFS

RE: Union Worker Communications, Inc.
Customer Proprietary Network Information Certification
EB Docket No. 06-36

Dear Ms. Dortch:

Union Worker Communications, Inc., by its undersigned attorneys, hereby submits its 2018 CPNI Compliance Certificate and Accompanying Statement certifying compliance with Section 64.2001 *et seq.* of the Commission's rules.

Please contact the undersigned should you have any questions or concerns at (269) 381-8893 extension 226 or patrick@crockerlawfirm.com.

Very truly yours,

CROCKER & CROCKER

Patrick D. Crocker

PDC/tlb

Enclosures

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

Date filed: February 14, 2019

Name of Company Covered by this Certification: Union Worker Communications, Inc.

Form 499 Filer ID: 823266

Name of Signatory: William VanderPloeg

Title of Signatory: President

I, William VanderPloeg, 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 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.

This Certification is dated this 14th day of February, 2019.

William VanderPloeg
President
Union Worker Communications, Inc.

ACCOMPANYING STATEMENT

Union Worker Communications, Inc.'s ("Union Worker") operating procedures ensure that Union Worker is in compliance with the requirements set forth in the Commission's CPNI rules as set forth in 47 C.F.R. Part 64, Subpart U (the "**CPNI Rules**") as follows:

- Union Worker's operating procedures prohibit the use, disclosure or release of CPNI, except as permitted or required under 47 U.S.C. § 222(d) and Rule 64.2005. Union Worker does not use disclose or permit access to CPNI for any purpose (including marketing communications-related services) and does not disclose or grant access to CPNI to any party (including to agents or affiliates that provide communications-related services), except as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.

- Union Worker's operating procedures prohibit the use of CPNI in sales or marketing campaigns. Union Worker does not use, disclose or grant access to CPNI for any purpose, to any party or in any manner that would require a customer's "opt in" or "opt out" approval under the Commission's CPNI Rules. Union Worker does not currently solicit "opt in" or "opt out" customer approval for the use or disclosure of CPNI.

- Union Worker takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Union Worker's operating procedures include safeguards designed to identify and protect against unauthorized use, disclosure or access to CPNI. Union Worker authenticates a customer prior to disclosing CPNI based on customer-initiated telephone contact or an in-store visit.

- Union Worker maintains a record of all instances where CPNI was disclosed or provided to third parties and where third parties were permitted access to CPNI. Records of all instances where CPNI was disclosed or provided to third parties, or where third parties were permitted access to CPNI, are maintained for a minimum of one year.

- Union Worker does not release call detail CPNI over the telephone, based on customer-initiated telephone contact, unless the customer first provides a password that is not prompted by Union Worker asking for readily available biographical information or account information or unless the customer is able to provide the relevant call detail information without Union Worker assistance. If a customer does not provide a password and is not able to provide the relevant call detail information without Union Worker assistance, Union Worker only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

- Union Worker provides customers with access to CPNI at Union Worker's retail locations only if the customer presents a valid photo ID and the valid photo ID matches an authorized name on the customer account. If a customer is not able to provide a valid photo ID, he or she may instead provide the account password in the same manner required for customer-initiated telephone contact. If a customer is not able to provide a valid photo ID or account password in connection with an in person inquiry, Union Worker only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

- Union Worker has established a system of passwords and password protection. For a new customer establishing service, Union Worker requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, Union Worker must first authenticate the customer without the use of readily available biographical information or account information, for example by calling the customer at the telephone Number of record or by using a personal identification number (PIN) or similar method to authenticate a customer.

- If a customer password is forgotten or lost, Union Worker uses a backup customer authentication method that is not based on readily available biographical information or account information.

- If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based on a customer-initiated telephone call by asking Union Worker to send the call detail information to an address of record or by Union Worker calling the customer at the telephone number of record. If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based on personal inquiry at a retail location by providing a valid photo ID that matches an authorized name on the customer account or by asking Union Worker to send the call detail information to an address of record or by Union Worker calling the customer at the telephone number of record.

- Union Worker has procedures and policies in place to notify a customer immediately when a password, customer response to a back-up means of authentication, address of record or other critical account information is created or changed.

- Union Worker does not currently provide online account access to customers.

- All Union Worker employees with access to or a need to use CPNI have been trained regarding Union Worker's operating procedures and as to when they are and are not authorized to use, disclose or permit access to CPNI. Union Worker's employees have been trained regarding the types of information that constitute CPNI and Union Worker's safeguards (such as employee restrictions, password protection, supervisory review, etc.) applicable to Union Worker's handling of CPNI. Union Worker's employee manual includes a disciplinary policy requiring compliance with Union Worker's operating procedures and sets forth penalties for noncompliance, up to and including termination of employment.

- Union Worker has appointed a compliance officer and established a supervisory review process regarding Union Worker's compliance with the Commission's CPNI Rules. Union Worker's operating policies require that employees confer with the compliance officer if they are unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI. Union Worker's operating policies require that the compliance officer confer with Union Worker's legal counsel if he or she is unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI.

- Union Worker's compliance officer has personal knowledge of Union Worker's operating procedures and is authorized, as an agent of Union Worker, to sign and file an annual CPNI compliance certification with the Commission.

- All Union Worker employees and the compliance officer are trained to identify and protect against activity that is indicative of pretexting. All Union Worker employees and the compliance officer are required to report any breach or potential breach of CPNI safeguards and/or any customer complaints regarding CPNI. In the event of a CPNI breach, Union Worker's operating procedures require compliance with the Commission's CPNI Rules regarding notice to law enforcement and customers. Union Worker must maintain records of any discovered breaches and notifications to the Secret Service and the FBI regarding those breaches, as well as the Secret Service and the FBI responses to such notifications, for a period of at least two years.