Mercury Wireless Inc.
1111 Main St. Suite 600
Kansas City, Missouri 64105

Annual 47 CFR § 64.2009(e) CPNI Certification

EB Docket 06-36

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

1. Date filed: 2/26/2019
2. Name of company(s) covered by this certification: Mercury Wireless, Inc.
3. Form 499 Filer ID: 829300
4. Name of signatory: Matthew G. Sams
5. Title of signatory: Chief of Staff, Corporate Secretary
6. Certification:

I, Matthew G. Sams, 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 CFR § 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, safeguards, record keeping, 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 CFR § 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.

Signed_____ [*Signature of an officer, as agent of the carrier*]

Attachments: Accompanying Statement explaining CPNI procedures

Mercury Wireless Inc.
1111 Main St. Suite 600
Kansas City, Missouri 64105

Mercury Wireless, Inc. CPNI Procedures

Mercury Wireless, Inc. and its subsidiaries Mercury Wireless Indiana, LLC and Mercury Wireless Kansas, LLC (collectively "Mercury Wireless") have implemented the following safeguards to ensure compliance with the CPNI rules of the Federal Communications Commission, 47 C.F.R. 64.2001 et seq:

(a) As an initial matter, the Mercury Wireless generally does not use CPNI for marketing purposes or for any other reason for which customer approval would be required under 47 C.F.R. § 64.2007(b). Because Mercury Wireless does not allow the use of CPNI for any reasons for which either opt-in or opt-out approval is required, such approval is not requested and all customers are treated as not providing such approval. Accordingly, the Company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.

(b) All Company personnel have been informed of when they are and are not authorized to use CPNI. Specifically, all Mercury Wireless personnel have been informed that CPNI is to be kept strictly confidential, is not to be used for marketing purposes, and that CPNI should not be provided to third parties except as required by law and when approved by a supervisor. In addition, all employees have been informed that disciplinary action would result from violating Mercury Wireless policy regarding CPNI.

(c) Mercury Wireless does not use CPNI for sales and marketing campaigns. Mercury Wireless does not disclose or provide CPNI to third parties, or allow access to CPNI by third parties, except as required by law. Mercury Wireless maintains records of all instances where CPNI was disclosed or provided to third parties.

(d) A supervisory review process is in place to ensure compliance with the Commission's rules for outbound marketing situations. Specifically, any proposed outbound marketing campaign, whether involving CPNI or not, would have to obtain supervisory approval.

(e) Mercury Wireless takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Specifically, Mercury Wireless has processes in place to properly authenticate a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or an in-person contact. Mercury Wireless does not have storefronts. All services are conducted over-the-phone, online, or at the customer's service location. Upon service installation, a VoIP customer's account information is verified by a valid photo ID, the customer establishes an email address of record, and the customer is provided a randomly generated password. A customer must provide this password in order to receive call detail information over the telephone. Customers may access CPNI online through a password-protected online.