BOOMERANG WIRELESS

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

EB DOCKET 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017.

Name of Company: Boomerang Wireless

Form 499 Filer ID: 827225

Name of Signatory: Scott Kokotan

Title of Signatory: CFO

I, Scott Kokotan, certify that I am an officer of Boomerang Wireless ("Boomerang" or the "Company") and acting as an agent of Boomerang Wireless, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Federal Communications Commission's ("Commission's" or "FCC's") Customer Proprietary Network Information ("CPNI") rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining that Boomerang Wireless procedures ensure that the Company is in compliance with the requirements set forth in sections 64.2001 *et seq.* of the Commission's rules. *See* 47 C.F.R. § 64.2009(e).

The Company has not taken any actions (*i.e.* instituted proceedings or filed petitions at either state commissions, the court system, or at the FCC) against data brokers during the above referenced certification period. Boomerang Wireless has no information outside of Commission Docket No. 96-115, or that is not otherwise publicly available (*e.g.,* through news media), regarding the processes pretexters are using to attempt to access CPNI. The steps the Company has taken to protect CPNI are described in the attached statement that summarizes the Company's operating procedures for compliance with the Commission's CPNI rules.

The Company has not received any customer complaints during the above referenced certification period concerning the unauthorized release of CPNI.

Date: 2/24/18

Signed: _____
Scott Kokotan

CFO

Boomerang Wireless

STATEMENT REGARDING OPERATING PROCEDURES
IMPLEMENTING 47 C.F.R. SUBPART U
GOVERNING USE OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)

Boomerang Wireless (the "Company") has established practices and procedures adequate to ensure compliance with Section 222 of the Communications Act of 1934, as amended, and the Federal Communications Commission's ("Commission's" or "FCC's") rules pertaining to customer proprietary network information ("CPNI") set forth in Sections 64.2001 – 64.2011 of the Commission's rules. This attachment summarizes those practices and procedures which are adequate to ensure compliance with the Commission's CPNI rules.

Safeguarding against pretexting

- The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI, including the authentication of customers prior to disclosing CPNI based on customer-initiated contacts. The Company is committed to notifying the FCC of any novel or new methods of pretexting it discovers and of any actions it takes against pretexters and data brokers.

Training and discipline

- The Company trains its supervisory and non-supervisory personnel in an effort to ensure that its employees, in accordance with FCC regulations: (a) understand what CPNI is, (b) join in and carry-out the Company's obligations to protect CPNI, (c) understand when they are and when they are not authorized to use or disclose CPNI, (d) obtain customers' informed consent as required with respect to its use for marketing purposes, and (e) keep records regarding receipt of such consent, customer complaints regarding CPNI and the use of CPNI for marketing campaigns.

- The Company's employees are required to review the Company's CPNI practices and procedures and to acknowledge their comprehension thereof.

- The Company has an express disciplinary process in place for violation of the Company's CPNI practices and procedures. The careless or intentional failure to comply with these practices and procedures may result in disciplinary action, up to and including discharge.

The Company's use of CPNI

- The Company may use CPNI for the following purposes:

  - To initiate, render, maintain, repair, bill and collect for services;
  - To protect its property rights; or to protect its subscribers or other carriers from fraudulent, abusive, or the unlawful use of, or subscription to, such services;
  - To provide inbound telemarketing, referral or administrative services to the customer during a customer initiated call and with the customer's informed consent.
  - To market additional services to customers that are within the same categories of service to which the customer already subscribes;
  - To market services formerly known as adjunct-to-basic services; and
  - To market additional services to customers *with the receipt of informed consent via the use of opt-in or opt-out, as applicable.*

- The Company does not disclose or permit access to CPNI to track customers that call competing service providers.

- The Company discloses and permits access to CPNI where required by law (*e.g.*, under a lawfully issued subpoena).

Customer approval and informed consent

- The Company does not use CPNI for marketing purposes. The Company also does not share, sell, lease, or otherwise provide CPNI to any of its affiliates, suppliers, vendors, or any third parties for any type of service for marketing purposes. If the Company changes this policy, it will implement a system to obtain approval and informed consent from its customers prior to the use of CPNI for marketing purposes. This system also will allow for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI. Records of approvals will be maintained for at least one year.

  One time use
  - After authentication, the Company may use oral notice to obtain limited, one-time approval for use of CPNI for the duration of a call. The contents of such notice will comport with Section 64.2008(f) of the FCC's rules.

Additional safeguards

- The Company requires supervisory approval for all marketing campaigns and maintains for at least one year records of such marketing campaigns, including a description of each campaign, the products offered as part of the campaign, and details of what information is used in connection with the campaign.

- The Company designates one or more officers, as an agent or agents of the Company, to sign and file a CPNI compliance certificate on an annual basis. The certificate conforms to the requirements set forth in Section 64.2009(e) of the FCC's rules.

- For customer-initiated telephone inquiries regarding or requiring access to CPNI, the Company authenticates the customer (or its authorized representative), through a dedicated account representative and a contract that specifically addresses the Company's protection of CPNI. In the event a customer does not have a dedicated account representative, the Company will authenticate the customer without prompting through the use of readily available biographical or account information, such as through the use of a pre-established password. If the customer cannot provide sufficient authentication, then the Company only discloses call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record.

- The Company does not permit online customer access to CPNI, nor does it have retail locations where customers may request access to CPNI.

- The Company notifies customers immediately of any account changes, including address of record, authentication, and password related changes.

- Within seven (7) days of a reasonable determination of a breach of CPNI, the Company will notify the U.S. Secret Service and the Federal Bureau of Investigation of the breach via the central reporting facility www.fcc.gov/eb/cpni. Customers will be notified after the seven (7) day period, unless the relevant investigatory party directs the Company to delay notification, or the Company and the investigatory party agree to an earlier notification. The Company will maintain a record of all CPNI security breaches, including a description of the breach and the CPNI involved, along with notifications sent to law enforcement and affected customers.