1001 Technology Drive
Little Rock, AR 72223

www.awcc.com

awcc
allied wireless communications corporation

February 10, 2014

VIA ECFS

Ms. Darlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, Suite TW-245
Washington D.C. 20554

Re: Annual 64.2009(e) CPNI Certification for 2013; EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e) of the Commission's Rules, Allied Wireless Communications Corporation hereby files its annual certification of compliance with the Commission's customer proprietary network information rules for the period January 1, 2013 through September 20, 2013.

Please contact the undersigned at 501-448-1249 should you have any questions.

Sincerely,

Rohan Ranaraja

Attachments:

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for Allied Wireless Communications Corporation

1. Date filed: February 10, 2014
2. Name of company covered by this certification: Allied Wireless Communications Corporation (see attachment)
3. Form 499 Filer ID: 828499 (see attachment)
4. Name and title of signatory: Wade McGill, Chief Administrative Officer
5. Period covered by this certification: January 1, 2013 through September 20, 2013 ("Relevant Period")
6. Certification:

I, Wade McGill, 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, as described in Sections A through J of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("Statement"), 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, including an explanation of actions taken against data brokers and a summary of customer complaints received during the Relevant Period covering the unauthorized release of CPNI.

W. McGill

Wade McGill
Chief Administrative Officer

Attachments: Companies covered by Annual CPNI Certification
Statement of Operating Procedures

COMPANIES COVERED BY ANNUAL CPNI CERTIFICATION OF ALLIED WIRELESS COMMUNICATIONS CORPORATION

Allied Wireless Communications Corporation (828499)
Georgia RSA #8 Limited Partnership (806211)

STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION FOR THE PERIOD JANUARY 1, 2013 TO SEPTEMBER 20, 2013

The following statement submitted on behalf of Allied explains how the operating procedures of Allied ensured that it was in compliance with the Commission's CPNI rules, as referenced herein and set forth in 47 C.F.R. Subpart U.

A. CPNI Use and Customer Approval

In accordance with 47 CFR 64.2005(a), Allied used CPNI internally for the purpose of providing a customer with the requested service and for marketing service offerings within the categories of service to which the customer subscribed from Allied. During the Relevant Period, Allied offered CMRS and information services. Consistent with 47 CFR 64.2005(b), Allied did not use, disclose, or permit access to CPNI to market telecommunications service offerings outside the category of service to which the customer subscribed. Allied used CPNI derived from the provision of CMRS for the provision of CPE and information services. Allied did not solicit customer consent to use CPNI in a manner that was beyond its then existing service relationship and Allied did not consider its customer to have granted approval for such CPNI use. As a result, the requirements contained in the revised section 64.2007(b) (Use of Opt-Out and Opt-In Approval Processes) pertaining to the approval process applicable to using customer's individually identifiable CPNI for marketing communications-related services to such customers did not apply to Allied's operational use of CPNI during the Relevant Period.

B. Sales and Marketing Campaigns

Pursuant to 47 CFR 64.2009, Allied reviewed sales and marketing campaigns that used CPNI. All such campaigns were conducted to market services within the category of service to which the customer subscribed from Allied in accordance with 47 CFR 64.2005(a). Allied did not engage in cross service marketing campaigns. In addition and consistent with 47 CFR 64.2009(d), Allied had a supervisory review process to evaluate the proposed use of CPNI in outbound marketing campaigns. Allied restricted the ability to create marketing campaigns in order to ensure compliance with the CPNI rules. The persons with authority to approve campaigns which used CPNI were previously authorized employees.

Consistent with 47 CFR 64.2009(c), Allied maintained records of the campaigns which used CPNI that were conducted by authorized personnel. These records contain a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. This information is retained for at least one year.

C. Training and Disciplinary Process

Allied personnel and agents were trained as to when they were and were not authorized to use CPNI and Allied's Customer Privacy Policy expressly established a disciplinary process applicable to employees and agents in the event it was determined that such policy had been violated. A violation of the policy and failure to protect customer information may lead to disciplinary action, up to and including termination.

D. Security Governance

Allied maintained policies, procedures, internal controls and systems designed to protect all of the data collected, generated, created, stored, managed, transmitted or otherwise handled by Allied employees.

E. Billing Records, Network Records, and Information

Allied maintained billing detail data, call detail data, and network record data in applications secured by networks, systems, policies and processes designed to control, monitor, and limit access to authorized users with legitimate business needs. Allied's corporate security team reviewed new applications and enhancements for compliance with existing security practices, which included requirements for access and authentication controls.

F. Data Centers

All data centers had processes and procedures in place for controlling physical access into the data centers along with controlling system access. Compliance with security policies was reviewed by Allied's Information Technology Security Manager during the Relevant Period for its systems.

G. Safeguards on the Disclosure of CPNI

(1) Safeguarding CPNI

Allied's account verification policy established the circumstances and limitations under which Allied call center and retail employees were allowed to disclose CPNI. These employees were monitored for compliance with Allied's account verification procedures.

Allied employees were trained to keep sensitive customer data strictly confidential and suspected breaches of customer confidentiality were investigated by corporate security teams. In addition to investigating reported incidents, security teams periodically conducted reviews of various systems to identify potential unauthorized access to customer data. Allied required newly-hired employees to sign an "Employee Agreement on Non-Disclosure and Non-Solicitation," which prohibited employees from disclosing information that was confidential to any third party. Confirmed unauthorized disclosures of customer information were subject to discipline, up to and including termination and referrals to law enforcement authorities where

deemed appropriate. Policies, practices, and technologies were used to limit employee access to customer records on a business need basis.

Allied's privacy statement described how Allied used, maintained and protected customer information, including CPNI. During the Relevant Period, this statement was available to all customers at www.alltelwireless.com by clicking on "Privacy Statement" at the bottom of Allied's home page. In addition, Allied's contracts with independent contractors that had access to confidential customer data were required to contain safeguards necessary to protect that data.

(2) Telephone Access to CPNI

By policy, reinforced with training and monitoring, Allied customer service representatives were prohibited from disclosing call detail (as defined in 47 CFR 64.2003(d)) over the telephone unless the customer service representative called the customer at the telephone number of record (as defined in 47 CFR 64.2003(q)). A customer service representative was allowed to assist the customer in the event an authenticated customer first identified the call to the representative without assistance during a call initiated by the customer. Upon request, Allied would mail a copy of the call details to the customer's address of record. In the event a customer's address of record had changed in the thirty days prior to the telephone request, Allied did not mail the required call detail. Instead, such customer is allowed to utilize online or in-store access. Allied's policy did not permit faxing of call detail.

(3) Online Access to CPNI

Allied maintained an online account retrieval system called "My Account" whereby Allied customers could register their account and subsequently login to access their account information and CPNI only after providing a valid password. During the Relevant Period, Allied's operating procedures were adequate to ensure compliance with the CPNI rules related to online access to CPNI, including a requirement that all wireless phone customers who register for My Account receive a text message to the designated handset on the account being registered. Pursuant to these procedures, a code in the text message would be required to complete the registration process.

Allied customers who wanted online access to their account information and CPNI first needed to register their account on My Account. Prior to beginning the registration process, customers were required to provide Allied their mobile number. The registration process required customers to: (1) provide their name; (2) create a unique user identification; (3) create a password; and (4) provide their electronic mail address. Wireless phone customers were sent a text message containing a unique code to their handset which was then used to complete the My Account registration process. Thereafter customers were required to utilize their user identification and password for online access to CPNI.

Additionally, Allied provided all customers the ability to block online access to their account and CPNI.

(4) Establishment of a Password and Back-Up Authentication Methods for Lost of Forgotten Passwords

Allied made available a backup authentication method for wireless phone customers who had forgotten their My Account password. This backup authentication method did not prompt the customer for readily identifiable biographical or account information. If the wireless phone customer did not provide the correct response for the backup authentication method, the customer was sent a code via text message to their handset. The customer was required to provide this code to Allied prior to establishing a new password.

(5) Notification of Account Changes

Allied immediately notified customers via text message to their handset or United States mail to their address of record, when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record was created or changed. Allied did not reveal the changed information.

(6) In-Store Access to CPNI

Allied required customers to present valid photo identification and verified that identity matched the account information prior to disclosing CPNI at an Allied retail location and at Allied agent retail locations.

H. Notification of CPNI Security Breaches

Allied's existing processes ensured compliance with the CPNI rules. In the event of a confirmed CPNI breach, Allied has established procedures to notify customers in accordance with the CPNI breach notification rules.

I. Summary of Customer Complaints Regarding the Unauthorized Release of CPNI

During the Relevant Period, Allied did not receive customer complaints concerning the unauthorized release of CPNI.

J. Action Taken Against Data Brokers

During the Relevant Period, Allied did not initiate any action against data brokers.