

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

SureWest Wireless

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 1, 2008

Name of company covered by this certification: SureWest Wireless

Form 499 Filer ID: 819194

Name of signatory: Fred Arcuri

Title of signatory: Sr. Vice President/Chief Operating Officer of SureWest Communications, parent company of SureWest Wireless

I, Fred Arcuri, 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed: 

Statement of CPNI Operating Procedures and Policies

SureWest Wireless (the "Company") has operating procedures designed to ensure that the Company is in compliance with the FCC's Customer Proprietary Network Information ("CPNI") rules.

1. The Company has implemented a system designed to verify the status of and protect a customer's CPNI. Because the Company does not use CPNI in marketing or sale of services, the customer's CPNI approval status is always considered to be "do not use," except for any purposes which are permitted under law without customer prior approval, such as for maintenance of a customer's current services, and prevention of fraudulent, abusive or unlawful use of telecommunications services. The Company does not share CPNI between affiliates, nor does it make CPNI available to third party vendors.
2. Company personnel are trained specifically regarding federal (47 U.S.C. Section 222 and 47 C.F.R. Part 64, Subpart U) and California (Public Utilities Code Section 2891) requirements for protection and use of CPNI. This information is posted in the Company's personnel Knowledge Management System that is used when discussing information with a customer regarding their service. Company personnel are subject to disciplinary action for failure to comply with CPNI rules.
3. Should the Company ever utilize CPNI in any sales or marketing campaigns, or disclose CPNI to third parties, the Company would maintain records of all such instances of use or disclosure. These records would include a description of the sales or marketing campaign and a record of all the customers whose CPNI were used for the campaign, or disclosed to a third party. The records would be maintained for at least one year.
4. The Company has established a supervisory review process regarding carrier compliance with the CPNI rules. Supervisors in the call center are required to monitor calls randomly to assure all procedures are being adhered to.
5. The Company will provide written notice to the FCC within five business days of any instance where the required opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

6. The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to customer CPNI. The Company releases CPNI to customers through in-store contact only with a valid photo ID or password. The Company has implemented a password system for the release of call detail records requested on customer-initiated telephone calls. If a customer does not provide a password, the Company will only release call detail information by sending it to an address of record associated with the customer's account for at least 30 days, or by calling the customer at the telephone number of record. The Company has implemented mandatory password protection for online account access that does not use readily available biographical information. Customers are immediately notified at the telephone number 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 is created or changed.

7. The Company will notify law enforcement of a breach of its customers' CPNI no later than seven business days after a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service and the Federal Bureau of Investigation.