

**Annual 47 C.F.R. S: 64.2009(e) CPNI Certification**  
**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for:	<b><u>2018 covering the prior calendar year 2017</u></b>
1. Data filed:	<b><u>02/27/2018</u></b>
2. Name of company covered by this certification:	<b>Consumer Cellular, Inc</b>
3. Form 499 Filer ID:	<b><u>824854</u></b>
4. Name of signatory:	<b><u>Jill Leonetti</u></b>
5. Title of signatory:	<b><u>Treasurer</u></b>
6. Certification:	

I, Jill Leonetti, certify that I am an officer of Consumer Cellular, Inc , being its Treasurer, (the company named above, herein referred to as "the company"), 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. S: 64.2001 et seq., which is a subpart to implement **section 222 of the Communications Act of 1934 as amended, 47 U.S.C. 222.**

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** (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 received no 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.

Signed



The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI, zero number of customer complaints received related to unauthorized access to CPNI, and zero number of incidents of unauthorized disclosure of CPNI. Here is the broken down by category or complaint as follows:

- |      |   |                            |
|------|---|----------------------------|
| (1). | Instances of improper access by employees:  | <u><b>0 complaints</b></u> |
| (2). | Instances of improper disclosure to individuals not authorized to receive the information:                | <u><b>0 Complaints</b></u> |
| (3). | Instances of improper access to online information by individuals not authorized to view the information: | <u><b>0 Complaints</b></u> |

If it was affirmative, above, the company would have provided summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

The company is aware of "Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, CC Docket No. 96-115; WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007)("EPIC CPNI Order"). See 47 U.S.C. S: 222".

**The company understands "47 C.F.R. S: 64.2009(e) in that it states:**

- (1). "A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis.
- (2). That the officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart.
- (3). That the carrier must provide a statement accompanying the certification explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart.
- (4). That the carrier must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.
- (5). That this filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year."

Signed



### Attached Accompanying Statement Explaining CPNI Procedures

The following are the measures put in place by the carrier (herein referred to as "the company") to protect CPNI from pretexting. The company understands that the three common types of "pretexting" are **identity theft, selling personal data for profit without authorization by the owner or using some other method for snooping for information whose release was not authorized by the owner of the information.**

- I. Pretexting via identify theft
  - (A). Identify theft via theft of physical hardware containing CPNI Data  
**Guarding Measures:**  
**The company utilizes physical security such as locks and security surveillance to protect physical hardware and limits physical access to authorized personnel. Portable hardware such as laptops have security features that provide additional security, and CPNI data is not stored on computers or laptops.**
  - (B). Identify theft via hacking/virtual intrusion of systems that carry CPNI  
**Guarding Measures:**  
**The company utilizes security software to detect and prevent unauthorized access via hacking and other virtual methods.**
- II. Pretexting via some other method for snooping for information whose release was not authorized by the owner.
  - (A). Snooping via social engineering/ impersonation/ false identification  
**Guarding Measures:**  
**The company's customer service personnel (the individuals most likely to be the targets of social engineering) have specific policies that they must follow to identify that they are in contact with the owner of the CPNI data prior to discussing or revealing CPNI.**
  - (B). Snooping by personnel not authorized to access data  
**Guarding Measures:**  
**The company limits access of CPNI to authorized personnel only.**
- III. Pretexting by selling CPNI for profit without authorization by the owner
  - (A). Selling CPNI data by the company with other companies  
**Guarding Measures:**  
**The company does not share CPNI data with other companies for marketing/profit purposes.**
  - (B). Sharing CPNI data for profit/marketing purposes by the company with sister companies, subsidiaries, parent companies or joint venture entities.  
**Guarding Measures:**  
**Not Applicable**