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

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2018

Date filed: March 1, 2019

Name of company covered by this certification: United States Cellular Corporation and its affiliates listed in Attachment A

Form 499 Filer ID: See Attachment A

Name of signatory: Steven T. Campbell

Title of signatory: Executive Vice President - Finance, Chief Financial Officer and Treasurer

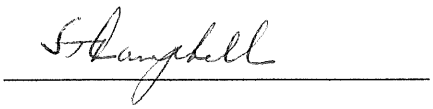
I, Steven T. Campbell, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *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 (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year.

The company received 141 customer complaints during 2018 that alleged unauthorized release of CPNI. This number of complaints is from a subscriber base of approximately 5,137,000 subscriber lines. Of the 141 complaints, 108 related to alleged instances of improper access, use, or disclosure of CPNI by employees (19% of which alleged unauthorized disclosure by specific employees), 10 related to improper access to online information by unauthorized individuals, and 23 related to various other instances of improper disclosure to unauthorized individuals. Approximately 74% of these complaints appear to relate to a personal issue between the involved individuals, such as a domestic dispute. Of the 141 customer complaints received, 58 were determined to be breaches of customers' CPNI and subsequently were reported to the United States Secret Service and Federal Bureau of Investigation through the Commission's central reporting facility.

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 

Steven T. Campbell
Executive Vice President – Finance, Chief Financial Officer and Treasurer
United States Cellular Corporation

Attachment A
Company Names and Filer ID

| Filer ID | Company Name | FEIN |
|---|---|---|
| 802587 | USCOC of Greater North Carolina, LLC | 36-3779831 |
| 802608 | California Rural Service Area #1, Inc. | 39-1740935 |
| 802611 | USCOC of Pennsylvania RSA #10-B2, Inc. | 39-1876663 |
| 802614 | Hardy Cellular Telephone Company | 31-1266169 |
| 802623 | Vermont RSA No. 2-B2, Inc. | 39-1737238 |
| 802641 | USCOC of Greater Iowa, LLC | 26-3769148 |
| 802644 | Cedar Rapids Cellular Telephone, L.P. | 36-3850690 |
| 802647 | Bangor Cellular Telephone, LP | 36-3880521 |
| 802685 | USCOC of Cumberland, Inc. | 36-3862875 |
| 802692 | Kansas #15, LP | 34-1675512 |
| 802704 | USCOC of LaCrosse, LLC | 36-3553841 |
| 802716 | Tennessee RSA No. 3 Limited Partnership | 62-1461122 |
| 802722 | United States Cellular Operating Company of Knoxville | 62-1147327 |
| 802731 | USCOC of South Carolina RSA #4, Inc. | 39-3811996 |
| 802737 | Yakima MSA Limited Partnership | 48-1066533 |
| 802743 | Dubuque Cellular Telephone, L.P. | 36-3880530 |
| 802746 | Farmers Cellular Telephone Company, Inc. | 42-1334334 |
| 802749 | Iowa RSA No. 9 Limited Partnership | 36-3668199 |
| 802755 | Iowa RSA No. 12 Limited Partnership | 36-3704891 |
| 802758 | United States Cellular Operating Company of Medford | 36-3584090 |
| 802761 | McDaniel Cellular Telephone Company | 93-0996859 |
| 802764 | USCOC of Washington 4, Inc. | 36-3645818 |
| 802767 | Oregon RSA #2, Inc. | 39-1669888 |
| 802779 | Western Sub-RSA Limited Partnership | 36-3804455 |
| 802785 | USCOC of Oregon RSA #5, Inc. | 39-1735612 |
| 802794 | USCOC of Greater Missouri, LLC | 36-3623765 |
| 802821 | Indiana RSA No. 5 Limited Partnership | 35-1805733 |
| 802824 | Indiana RSA No. 4 Limited Partnership | 35-1805731 |
| 802833 | United States Cellular Telephone Company (Greater Knoxville), L.P. | 36-3332471 |
| 802849 | Texahoma Cellular Limited Partnership | 75-2494073 |
| 802851 | NH #1 Rural Cellular, Inc. | 36-3717952 |
| 802860 | Maine RSA #1, Inc. | 36-3717943 |
| 802863 | USCOC of Greater Oklahoma, LLC | 36-3811995 |
| 807699 | USCOC of Virginia RSA #3, Inc. | 72-1176997 |
| 817226 | Madison Cellular Telephone Company | 91-1387617 |
| 817230 | Kenosha Cellular Telephone, L.P. | 39-1757974 |
| 817232 | Racine Cellular Telephone Company | 91-1431833 |
| 818126 | Jacksonville Cellular Telephone Company | 56-1585202 |
| 821504 | USCOC of Richland, Inc. | 36-4404449 |
| 821506 | Maine RSA #4, Inc. | 36-3717946 |
| 821508 | United States Cellular Operating Company LLC | 36-3363349 |
| 821600 | USCOC of Central Illinois, LLC | 68-0231012 |
| 823622 | USCOC of Rochester, Inc. | 54-2042835 |
| 825693 | USCOC Nebraska/Kansas, LLC | 20-3466461 |

**2018 Statement of CPNI Compliance Procedures**

United States Cellular Corporation on behalf of its CMRS operating affiliates (collectively "U.S. Cellular" or the "Company") has established operating procedures that are adequate and intended to ensure compliance with the requirements of Section 222 of the Telecommunications Act of 1996, as amended, and with the implementing rules adopted by the Federal Communications Commission at 47 C.F.R. Part 64, Subpart U ("CPNI Rules"). Unless otherwise stated, this statement reflects the operating procedures in place as of December 31, 2018.

Responsibility for the overall compliance of the Company with the CPNI requirements lies with the Director, Privacy and Senior Counsel who reports to the Vice President, Legal and Regulatory Affairs. Among other things, the Director, Privacy and Senior Counsel is required to do a quarterly assessment of the status of U.S. Cellular's compliance efforts with the CPNI Rules and other privacy protection initiatives. The Company has a process that supports management's ability to have personal knowledge that the operating controls and procedures that have been established in their respective areas of responsibility are in place and working. This process requires that key managers ("Control Owners"), whose organizational responsibilities include the oversight of specific operating procedures and controls that support compliance with the CPNI Rules, test controls and procedures and submit reports to their manager ("Process Owners") on the results of their findings. These reports are subsequently submitted by the Process Owners to the Director, Privacy and Senior Counsel along with an accompanying statement that the Process Owners have reviewed and approved the reports. This process is updated on an ongoing basis as controls and procedures change over time.

U.S. Cellular has implemented the following procedures in order to protect the CPNI of U.S. Cellular's customers:

**Permission Notice for use of CPNI by Agents and Affiliates:**

Currently, U.S. Cellular exclusively provides CMRS services. Thus, every marketing interaction that it has with customers is exclusively "within category" as the FCC has defined that term and for which no explicit permission from customers is required for the use of their CPNI by the Company for marketing purposes. U.S. Cellular also has an agent distribution channel ("Agent") for both in-bound and out-bound customer interactions and relationships with other affiliates ("Affiliates") who may from time to time have a need to access customer information for marketing telecommunication services to customers. With respect to the sharing of CPNI with Agents and Affiliates for marketing purposes, U.S. Cellular obtains permission from customers using the FCC sanctioned Notice and Opt-Out method as follows:

- A CPNI Notice is included in each postpaid customers' bill which also provides a link to the additional CPNI information ("CPNI Notice") available on the web page. New postpaid customers will receive the CPNI Notice on their initial bill

and then every month thereafter. Copies of the CPNI Notice are posted on U.S. Cellular's website.

- Postpaid business and government customers that receive electronic billing will continue to receive the CPNI Notice in the mail shortly after establishing service. Prepaid customers are sent a text message containing a link to a web page providing them with the CPNI Notice shortly after establishing service.

- Although not required by the CPNI rules, all mailed notices are in dual language (English and Spanish) and the contents of the Notice satisfy the substantive requirements of 47 C.F.R. §64.2008 (2)(c)(1) through (10).

- A campaign planning and management system is used to plan for and generate campaigns for CPNI Notices to those prepaid customers, and business and government customers that receive electronic bills no less than every 2 years.

- Customers are given a minimum of 33 days to respond to the CPNI Notice before they are considered to have provided implied consent to allow U.S. Cellular to share their CPNI with Agents and Affiliates for the purposes of marketing the Company's or its affiliated companies' products and services. The billing system maintains the CPNI status of a customer as being in the initial notification waiting period, having opted out, or having implied consent. Agents have received specific written direction that they are not to access any CPNI from new customers for marketing purposes until the initial notification waiting period has passed for determining the customer's CPNI permission status.

- An Interactive Voice Response ("IVR") system with a dedicated toll-free number is available on a 24/7 basis (except for minimum downtime for required maintenance in off-hours) for customers to contact in order to opt-out. Customer calls are automatically routed to a call center or voicemail box in the event that the IVR is unavailable. Customers may also visit a Company owned retail store or call Customer Service to opt-out. There is no additional cost to the customer to use any of these opt-out methods.

- A process is in place for the monitoring, reporting, and escalation of the IVR system's availability to support customer opt-out calls.

**Approval for use of CPNI:**

- Customer elections to opt-out from granting U.S. Cellular permission to allow its Agents and Affiliates to use their CPNI for the purposes of marketing the Company's products and services remain in effect until a customer requests that such election be revoked.

- Records of customer opt-out elections are maintained in U.S. Cellular's customer information billing system for at least as long as customers remain in active status.

- Customers' opt-out status is automatically updated daily in the campaign management system used by the internal U.S. Cellular marketing employees who prepare marketing campaigns.

**General Safeguards for use of CPNI**

- All Company and Agent employees are required to complete CPNI training during their orientation period. Additional policy and procedures training is provided to front line employees. All employees are required to complete a refresher course annually following the calendar year in which they are hired.

- U.S. Cellular has an express disciplinary process in place to protect customer privacy and CPNI. Although employees are subject to progressive disciplinary actions for failure to comply with the Company's policies pertaining to customer privacy and CPNI; providing call and message detail to a customer that has not been properly authenticated or to an unauthorized party subjects employees to significant disciplinary action up to and including immediate termination. Agents of the Company are informed in writing of their obligations to protect customer privacy and CPNI and are subject to disciplinary actions including possible contract termination for non-compliance with the terms of their agreements.

- Company and Agent direct marketing and market research campaigns to existing customers using CPNI are documented, reviewed, and approved by a manager with supervisory authority. U.S. Cellular policy requires that the campaign records be stored for a minimum of one year.

**Authentication**

- In order to streamline the authentication process, USCC has implemented automated authentication procedures through the IVR system. Under the process, customers have the ability to electronically authenticate themselves over the phone prior to the call being routed to an associate. Dependent upon account or customer-type, the authentication process varies slightly. First, the IVR prompts customers to key-in their PIN. Second, if customers do not input their PIN, calls are routed to an employee and customers are asked for their full name and PIN. If customers cannot provide that information, employees request the answer to a previously answered security question. Finally, if customers cannot answer the security question, customers can authenticate through a one-time PIN tool that allows the employee to send the customer a one-time PIN to a telephone number on the account after the customer has been verified through providing the social security number or the tax ID associated with the account. Those customers that

cannot be authenticated through any of the methods identified above are required to authenticate in-person at a retail store.

- As an additional security measure, a systematic pop-up screen reminds call center employees on each incoming call to authenticate a customer before providing any confidential personal information including CPNI. The employee must close the pop-up screen in order to obtain access to any customer record. A failure by an employee or Agent to authenticate a customer prior to disclosing, adding or changing customer account information, including but not limited to CPNI, subjects that employee or Agent to U.S. Cellular's disciplinary process.

- U.S. Cellular policy requires that its customers be authenticated by employees and Agents with a valid government issued photo ID before providing CPNI during an in-store contact at retail stores.

- Employees and Agents are authenticated when requesting CPNI over the phone on behalf of customers by providing a Security Word in addition to other personal identification information. The Security Word is changed frequently.

- U.S. Cellular policy prohibits employees from using readily available biographical information ("RABI") or account information to prompt customers for their passwords.

- U.S. Cellular policy prohibits employees from providing call or messaging detail over the phone even if the customer has been properly authenticated. U.S. Cellular policy requires that requests for call or messaging detail from customer-initiated phone contacts by postpaid customers be fulfilled by mailing the information to the address of record for the account.

- Registration for an online account with access to billing information and CPNI requires a unique PIN in addition to account information and does not rely solely on RABI or account information. The PIN number is sent via a text message to a telephone number of record selected by the customer. Subsequent access to CPNI online by a customer requires a unique username and password which is established by the customer. Back up authentication methods for lost or forgotten passwords do not use RABI or account information. Customers who cannot provide the proper responses to back up authentication questions are sent a temporary password to the email address of record for their account that they may use to reset their username or password. Customers may also go to a retail store and authenticate with a valid government issued photo ID in order to reset their username or password.

**Notification of account changes**

- A text message is sent to a telephone number of record to notify the customer when an online account, password, email address, or response to a back-up means of authentication for lost or forgotten password is created or changed. A letter is sent to the postal address of record when a postal address of record is created or changed for a postpaid customer.

**Notice of unauthorized disclosure of CPNI**

- A Privacy Incident Response Plan including a Privacy Incident Response Team ("PIRT") has been created to handle the internal investigation and reporting of events that may result in reportable breaches of CPNI. Information about how to report such events is readily available to all employees on the Company's internal website and in the Company's training courses.

**Other measures to protect CPNI**

- U.S. Cellular proactively alerts employees in sales channels and call centers when suspicious pretexting attempts are identified. Alerts are given to the respective retail stores in the area or across call center departments to alert them to this activity.

- There are formalized processes that address the management of access to the centralized customer management system that stores CPNI. These processes address:
    - Requesting and approving access to applications that access CPNI, including administrative access. This process is partially automated.
    - Periodic employee entitlement reviews for appropriate level of access, including administrative access. This includes protection against the accumulation of access rights during employee role transfers.
    - Removal of access rights for terminated employees.
    - Separate developer access procedures requiring higher level of approval that are routinely reviewed.
    - Periodic auditing of these processes.

- Vulnerability scans on externally-facing and internal U.S. Cellular systems are performed routinely. These activities attempt to discover vulnerabilities that may be exploited to compromise the security of the internal U.S. Cellular network and the customer data it contains. Vulnerabilities (including systems patching) are assessed, prioritized, and scheduled for remediation as appropriate.

- Next-generation firewalls are used to detect application-specific attacks and enforce an application-specific granular security policy on the network perimeter. Application and threat signature databases are updated routinely. Layers of

firewalls also secure the demilitarized zone and internal systems. Firewalls restrict and filter connectivity to the systems that provide access to CPNI.

- Anti-virus software is installed on workstations to help protect against known viruses, worms, and Trojans.

All of the foregoing measures demonstrate that U.S. Cellular has established operating procedures that are adequate to ensure compliance with the FCC's CPNI Rules.