

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

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

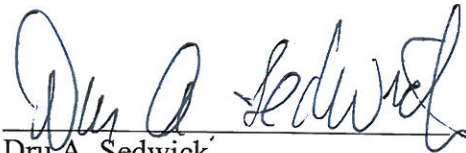
1. Date filed: March 1, 2018
2. Name of companies covered by this certification and Form 499 Filer IDs:  
**Armstrong Telecommunications, Inc. 822660**  
**Armstrong Digital Services, Inc. 825987**
3. Name of signatory: Dru A. Sedwick
4. Title of signatory: President
5. Certification:

I, Dru A. Sedwick, certify that I am President of Armstrong Telecommunications, Inc. and Armstrong Digital Services, Inc. (together, "Company"), and, acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures, as summarized in the attached statement, that are adequate to ensure compliance with the Commission's customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the of the Commission's rules, 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 received any customer complaints in the past calendar year concerning unauthorized release of CPNI. Company has not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission.

The Company hereby represents and warrants that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject the Company to enforcement actions.



Dru A. Sedwick

President

Armstrong Telecommunications, Inc.

Armstrong Digital Services, Inc.

Executed February 28, 2018

## **CPNI Compliance Policies of Armstrong Telecommunications, Inc.**

The following summary describes the policies of Armstrong Telecommunications, Inc. and Armstrong Digital Services, Inc. (including all employees, associates, and agents thereof, “Armstrong”) that are designed to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.*

CPNI is “(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”

Armstrong’s policy, administered by its CPNI Compliance Manager, Terry Dickerhoof, Vice President of Customer Service Operations & Billing, establishes the following parameters regarding the protection, use, and disclosure of CPNI:

### **1. USE, DISCLOSURE OF, AND ACCESS TO CPNI**

Armstrong may use, disclose, or permit access to CPNI without customer approval in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Armstrong, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; and to provide inside wiring installation, maintenance, or repair services; as expressly authorized by the customer; or as required by law.

Armstrong does not use CPNI for outbound marketing of service even within the same category of service that it provides to subscribers. Although current Armstrong policy is not to use CPNI in outbound marketing, in the event that any employee or agent wishes to use CPNI in such marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve a supervisor designated by the senior employee responsible for marketing and the CPNI Compliance Manager. If such use is approved, Armstrong shall modify these policies and conduct additional training as needed to assure compliance with the FCC’s rules.

Armstrong does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When Armstrong receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

## **2. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES**

Above and beyond the specific FCC requirements, Armstrong will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Armstrong's existing policies that would strengthen protection of CPNI, they should report such information immediately to Armstrong's CPNI Compliance Manager so that Armstrong may evaluate whether existing policies should be supplemented or changed.

### **(a) Establishment of Personal Identification Numbers**

Upon the establishment of a new account or at the customer's request, Armstrong will send a randomly-generated CPNI personal identification number ("PIN") to the customer's address of record.

### **(b) Inbound Calls to Armstrong Requesting CPNI**

Call Detail Information (CDI) includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call. Armstrong will not disclose CDI to an inbound caller unless the caller is authenticated as the customer by correctly providing the PIN with the account.

Armstrong may also send a copy of a bill or requested CDI to an address of record for the account, but only if such address has been on file with Armstrong for at least 30 days.

If an inbound caller is able to provide to the customer service representative (CSR) the telephone number called, the time of the call, and, if applicable, the amount charged for the call, exactly as that information appears in Armstrong's records, then the CSR is permitted to discuss customer service pertaining to that call and that call only.

CSRs require an inbound caller to authenticate their identity prior to revealing any CPNI other than CDI or account information to the caller.

### **(c) Online Accounts**

To access an online account from which a customer can access their CPNI, customer must enter the online password that they established at service initiation or that is sent to the customer's address of record upon request.

### **(d) In-Person Disclosure of CPNI at Armstrong Offices**

Armstrong may disclose a customer's CPNI to an authorized person visiting an Armstrong office upon verifying that person's identity through a valid, non-expired government-issued photo ID

(such as a driver's license, passport, or comparable ID) matching the customer's account information.

**(e) Notice of Account Changes**

Armstrong will send a notification to a customer's address of record immediately whenever a password, PIN, Security Question, online account, or address of record is created or changed, except for such events that occur during the period when the customer initiates service. When such a change is made to an address of record, the notice will be sent only to a pre-existing address of record. The notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Armstrong if they have any questions regarding the change.

**3. REPORTING CPNI BREACHES TO LAW ENFORCEMENT**

Any Armstrong employee that becomes aware of any breaches, suspected breaches or attempted breaches of CPNI must report such information immediately to the Armstrong CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Armstrong's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Armstrong's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

**(a) Identifying a "Breach"**

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If an Armstrong employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Armstrong's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. Armstrong's CPNI Compliance Manager will determine whether it is appropriate to update Armstrong's CPNI policies or training materials in light of any new information; the FCC's rules require Armstrong on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

**(b) Notification Procedures**

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. Armstrong's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

Armstrong will not under any circumstances notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below (a full business day does not count a business day on which the notice was provided). Federal law requires compliance with this requirement even if state law requires disclosure.

If Armstrong receives no response from law enforcement after the 7<sup>th</sup> full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Armstrong will delay notification to customers or the public upon request of the FBI or USSS. If the CPNI Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Armstrong still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

**4. RECORD RETENTION**

The CPNI Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Armstrong maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Armstrong later begins to use CPNI for outbound marketing of different categories of service to which the customer already subscribes, it will also keep a record for a period of at least one year, of supervisory review of marketing that proposes to use CPNI and records related to requests for customer approval to use or disclose CPNI.

Armstrong maintains a record of all customer complaints related to their handling of CPNI, and records of Armstrong's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that Armstrong considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Armstrong will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that

Armstrong has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Armstrong's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing 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. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

## **5. TRAINING**

All employees with access to CPNI receive a copy of Armstrong's CPNI policies and are informed that (i) Armstrong takes seriously the protection of its customers' CPNI, and any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Armstrong requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.