Annual 64.2009(e) CPNI Certification for 2019, Covering the Prior Year 2018

EB Docket 06-36

1. Date filed: March 1, 2019

2. Name of company(s) covered by this certification: AMCS LLC

3. Form 499 Filer ID: 832041

4. Name of signatory: Chris Vonderhaar

5. Title of signatory: Vice President

6. Certification:

I, Chris Vonderhaar, 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 CFR § 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, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken 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. Company has not discovered any information about the processes that pretexters are using to attempt to gain access to CPNI other than the information that already is contained publicly in this docket.

The company has not received 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 CFR § 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 

Attachments: Accompanying Statement

Statement Accompanying CPNI Certification for 2019, Covering the Prior Year 2018

EB Docket No. 06-36

AMCS LLC ("Company") does not use, disclose or permit access to, nor has it ever used, disclosed or permitted access to, Customer Proprietary Network Information ("CPNI") except as permitted or required under 47 U.S.C. Section 222 or the Commission's rules.

PERMISSIBLE USES OF CPNI

Company limits its use of CPNI unless necessary. Company may use, disclose, or permit access to CPNI for the permissible purposes enumerated in 47 U.S.C. Section 222 or the Commission's rules, including, but not limited to: (1) initiating, provisioning, rendering, and billing for telecommunications services; (2) protecting the Company's rights and property, and (3) protecting customers and other carriers from fraudulent, abusive or unlawful use of, or subscription to, its services. The Company does not use, disclose or permit access to CPNI to identify or track customers who call competing service providers.

USE OF CPNI FOR MARKETING PURPOSES

Currently, Company does not use CPNI to conduct outbound marketing or in connection with its sales and marketing campaigns outside of the category of Company's service to which the customer already subscribes. If, in the future, Company seeks to use CPNI for these purposes, Company will fully comply with the applicable Commission rules.

CPNI SAFEGUARDS

Company takes reasonable measures to discover and protect against attempts to gain against unauthorized access to CPNI. Company utilizes authentication procedures, without the use of readily available biographical information or account information, for in-coming calls and online account access to CPNI. Company requires customers to establish a password for all online accounts, and Company has implemented procedures to address lost or stolen passwords, which do not rely on the use of readily available biographical information or account information. Company notifies customers, via email, whenever certain account information, including password changes, is created or changed. For business customers who have specifically authorized release of CPNI pursuant to a procedure established by contract, Company may utilize authentication regimes other than those described in this section.

EMPLOYEE TRAINING/DISCIPLINARY PROCESS:

Company trains its personnel in the use of CPNI. Company also has implemented network security measures, pursuant to which Company personnel have access only to information that is necessary for their particular position; therefore, access to CPNI by Company personnel is established on a need-to-know basis. Company has a disciplinary process in place for violations of Company's data security policies.

DATA SECURITY BREACHES/REQUESTS FOR CPNI

Company has practices and procedures in place to notify customers, if permitted, and law enforcement, as required, of a security breach which results in the unauthorized access to, use or disclosure CPNI. Company will maintain a record of the notification in accordance with the Commission's rules.

Company has procedures in place for responding to requests for CPNI from any person other than the customer. It is Company's policy not to release any information to any person other than the customer's authorized representative absent a validly issued court order.