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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018

Date filed: February 27, 2019

Name of company covered by this certification:	T-Systems North America, Inc.
Form 499 Filer ID:	820820
Name of signatory:	Bertus Cilliers
Title of signatory:	Vice President Finance

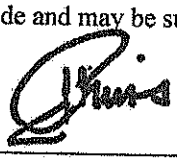
I, Bertus Cilliers, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et 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) 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.

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 be subject to enforcement action.

Signed 

Bertus Cilliers, VP Finance, T-Systems North America, Inc.

Date February 25, 2019

T-SYSTEMS NORTH AMERICA INC.
STATEMENT REGARDING CUSTOMER PROPRIETARY NETWORK INFORMATION OPERATING PROCEDURES

February 22, 2019

This statement is filed on behalf of T-Systems North America, Inc. ("TSNA" or "Company") pursuant to 47 C.F.R. § 64.2009(e) to demonstrate how TSNA's operating procedures are designed to ensure compliance with the Commission's CPNI rules.

Certification

TSNA requires a corporate officer to act as agent for the company and sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with applicable CPNI rules. TSNA's certifying officer relies in part upon information provided by corporate officers and managers directly responsible for implementing the Company's CPNI operating procedures.

TSNA CPNI Protection Policy

TSNA has implemented a CPNI Protection Policy Statement, which addresses, among other things, the policies and procedures the Company has implemented to safeguard its customer's CPNI. The TSNA Protection Policy Statement was delivered to all employees of TSNA, and explains, among other things, what constitutes CPNI, what requirements apply to the use and/or disclosure of CPNI, TSNA CPNI safeguards, and what kinds of record-keeping and reporting obligations apply to CPNI. The Policy is also provided to new employees as part of their orientation materials and included in the Employee Handbook.

TSNA CPNI Instruction Manual

TSNA has implemented a CPNI Instruction Manual. The TSNA Manual explains to its employees how to implement TSNA's CPNI Policies as outlined in the TSNA Protection Policy Statement. The Manual addresses the following topics:

- The process for verifying a customer's identity;
- What information, if any, can be disclosed to the customer upon a customer request;
- When TSNA employees may use CPNI for marketing purposes,
- What to do if a TSNA employee receives a request for CPNI from law enforcement or any other person other than the customer of record; and
- What to do in the event of CPNI security breach.

Use, Disclosure and Access to CPNI

TSNA does not use, disclose or permit access to its customers' CPNI except as any such use, disclosure or access is permitted by Section 222 of the Telecommunications Act of 1996. TSNA does

not use CPNI to market services to customers outside of the category of service to which the customer already subscribes. TSNA also does not share CPNI with its affiliates, or third parties for any marketing purposes. If, in the future, TSNA seeks to use CPNI to market services to customers that are outside of the category of service to which the customer subscribes or to share CPNI with affiliates or third parties, TSNA will provide notice to its customers advising them of their right to approve or disapprove of the proposed uses of CPNI. TSNA will maintain a list of customer preferences.

All marketing campaigns using CPNI must receive prior approval and must be conducted in accordance with the TSNA Policy Statement and CPNI Manual. TSNA will maintain records of all marketing campaigns that use CPNI in accordance with the FCC's rules.

Call Detail Information

TSNA has implemented a policy prohibiting the release of Call Detail Information to any customer during an in-bound call. If a TSNA employee receives a request for Call Detail Information, he/she may provide that information to the caller by sending the information to the address of record or calling the customer back at the telephone number of record. TSNA's policy on Call Detail Information does not allow an employee to disclose any Call Detail Information to the customer other than the Call Detail Information that the customer already has disclosed.

Safeguarding CPNI

TSNA takes the privacy and security of CPNI seriously. In addition to its Call Detail Information Policy, TSNA has established authentication procedures applicable to incoming calls. TSNA has also established detailed procedures for processing certain account changes, and requires the applicable personnel to notify customers immediately of such account changes. TSNA also has implemented network safeguards, including, but not limited to, encrypting certain data. TSNA does not have retail locations.

Employee Training

TSNA has engaged in targeted training of employees and contractors to communicate the proper use and maintenance of CPNI.

Employee Discipline Program

TSNA has a disciplinary process in place to address any noncompliance with Company policies, including policies concerning employee use of, access to, and disclosure of CPNI. An employee found to have violated TSNA's policies, including policies relating to use of, access to, and disclosure of CPNI, is subject to disciplinary action up to and including termination.

Notice of Security Breaches

Pursuant to TSNA policies, TSNA employees are required to notify their supervisor (who will notify the legal department) immediately if they discover a security breach that has resulted in the unauthorized use, disclosure, or access to CPNI. TSNA notifies the United States Secret Service and the Federal Bureau of Investigation as well as its affected customers of any breaches in accordance with 47 C.F.R. § 64.2011(e). TSNA maintains a record of all security breaches.