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 ~~22~~ 27, 2019

Name of company covered by this certification:	Deutsche Telekom North America, Inc.
Form 499 Filer ID:	826948
Name of signatory:	Kevin Mulholland
Title of signatory:	President and Chief Executive Officer

I, Kevin Mulholland, 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 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 _____

Kevin Mulholland, President and Chief Executive Officer

Date 2/27/19

DEUTSCHE TELEKOM NORTH AMERICA INC.
STATEMENT REGARDING CUSTOMER PROPRIETARY NETWORK INFORMATION OPERATING PROCEDURES

22 February 2019

This statement is filed on behalf of Deutsche Telekom North America, Inc. ("DTNA" or "Company") pursuant to 47 C.F.R. § 64.2009(e) to demonstrate how DTNA's operating procedures are designed to ensure compliance with the Commission's CPNI rules.

Certification

DTNA 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. DTNA's certifying officer relies in part upon information provided by corporate officers and managers directly responsible for implementing the Company's CPNI operating procedures.

DTNA CPNI Protection Policy

DTNA 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 DTNA Protection Policy Statement was delivered to all employees of DTNA, and explains, among other things, what constitutes CPNI, what requirements apply to the use and/or disclosure of CPNI, DTNA 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.

DTNA CPNI Instruction Manual

DTNA has implemented a CPNI Instruction Manual. The DTNA Manual explains to its employees how to implement DTNA's CPNI Policies as outlined in the DTNA 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 DTNA employees may use CPNI for marketing purposes;
- What to do if a DTNA 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

DTNA 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.

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

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

Call Detail Information

DTNA has implemented a policy prohibiting the release of Call Detail Information to any customer during an in-bound call. If a DTNA 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. DTNA'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

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

Employee Training

DTNA has engaged in company wide training of all employees and contractors to communicate the proper use and maintenance of CPNI.

Employee Discipline Program

DTNA 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 DTNA'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 DTNA policies, DTNA 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. DTNA 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). DTNA maintains a record of all security breaches.