Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018
EB Docket 06-36

1. Date filed: March 1, 2019

2. Name of company(s) covered by this certification: Genesys Telecom US, Inc.

3. Form 499 Filer ID: 830996

4. Name of signatory: William Dummett

5. Title of signatory: Chief Privacy Officer

6. Certification:

I, William Dummett, 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 the 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 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 William Dummett

Attachment: Accompanying Statement explaining CPNI procedures

GENESYS TELECOM US, INC.

2018 CPNI Compliance Statement of Operating Procedures

Genesys Telecom US, Inc. ("Company") submits this compliance statement as required by 47 C.F.R. §64.2009(e). During the 2018 reporting period, Company had in place a Customer Proprietary Network Information Policy ("CPNI Policy") that is sufficient to ensure compliance with the Commission's CPNI regulations.

General duty, training, and discipline

The CPNI Policy defines CPNI consistently with 47 C.F.R. § 64.2003, addresses proper handling and use of CPNI, imposes a duty on employees to safeguard CPNI, and provides that violations of the CPNI Policy will subject an employee to disciplinary action, up to and including immediate termination of employment.

Company makes CPNI available to employees only on a need-to-know basis. During the reporting period, Company provided a training on its CPNI Policy for employees who have access to CPNI.

Use of customer proprietary network information without customer approval (47 C.F.R. § 64.2005); Approval required for use of customer proprietary network information (47 C.F.R. § 64.2007); Notice required for use of customer proprietary network information (47 C.F.R. § 64.2008); Safeguards required for use of customer proprietary network information (47 C.F.R. § 64.2009)

Company does not use, disclose, or permit access to CPNI for marketing purposes except as permitted by Section 222 of the Communications Act or regulations implementing Section 222 of the Communications Act. Company does not disclose CPNI to third parties or permit third parties to access or use CPNI, except as permitted by Section 222 of the Communications Act or regulations implementing Section 222 of the Communications Act.

Safeguards on the disclosure of customer proprietary network information (47 C.F.R. § 64.2010)

Company protects against attempts to gain unauthorized access to CPNI and authenticates a customer prior to disclosing CPNI. It does not operate retail locations; accordingly, its customers have no in-store access to CPNI. For access to CPNI over the telephone, Company authenticates a customer through use of a password that is not prompted by the carrier asking for readily available biographical information or account information, or as otherwise provided in 47 C.F.R. § 64.2010(b). If the customer does not recall his or her password, Company authenticates the customer without using readily available biographical information or account information.

Customers may also access their CPNI online and establish a password for future access only after being authenticated without using readily available biographical information or account information. After initial authentication, customers may access CPNI online only by providing their pre-established password, which is not prompted by Company asking for readily available biographical information or account information. Customers that have lost or forgotten their passwords may retrieve their passwords by contacting Genesys Customer Care, which does not involve the use of readily available biographical information or account information. If a customer cannot provide the correct password or the back-up method, the customer must be re-authenticated and must establish a new password.

The CPNI Policy requires immediate customer notification whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notice does not reveal the changed information and is sent to the existing telephone number of record, by mail to the existing physical address of record, or by e-mail to the existing e-mail address of record, and not to any address or number that has been changed.

Notification of customer proprietary information security breaches (47 C.F.R. § 64.2011)

Company is unaware of any breach of CPNI during the reporting period.

The CPNI Policy requires notification of relevant law enforcement agencies and customers in accordance with FCC rules in the event of a breach of CPNI. Company will maintain records of any

breaches discovered, notifications made to law enforcement, and notifications made to customers. These records will include, where 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. The Company will maintain these records for 2 years.

Any actions against data brokers or customer complaints (47 C.F.R. § 64.2009(e))

Company has not taken any actions against data brokers in the preceding year. Company has not had any customer complaints concerning the unauthorized release of CPNI.

Instances where opt-out mechanisms do not work properly (47 C.F.R. § 64.2009(f))

Company has not not faced any instance where the opt-out mechanisms did not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

Signed William Dummett

William Dummett, Chief Privacy Officer