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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2017

Date filed: March 8, 2018

Name of company covered by this certification: US Telephone & Telegraph

Form 499 Filer ID: 830686

Name of signatory: Tran Van Son

Title of signatory: Manager

I, Tran Van Son, 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 Customer Proprietary Network Information (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 the company with either state commissions, the court system, or the Commission) against data brokers in the past year. I acknowledge that companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI, and I have no such information to report at this time.

The company has not received any customer complaints in the past year concerning the unauthorized release of or access to CPNI and I hereby acknowledge that if the company does receive any such complaints, it must provide that information to the Commission, including the number of customer complaints the company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.

Tran Van Son

Tran Van Son, Manager

Statement Accompanying CPNI Certificate EB Docket No. 06-36

US Telephone & Telegraph (the "Company") does not use, disclose or permit access to Customer Proprietary Network Information ("CPNI") except as permitted or required by law pursuant to 47 U.S.C. § 222. The safeguards set forth in Sections I and J below are followed by the Company, and, to the extent that the Company finds it necessary to use, disclose or permit access to CPNI, the operating procedures in Sections A-H below are observed.

A. Definitions. The terms used in this Statement have the same meaning as set forth in 47 §64.2003.

B. Use of CPNI. It is the Company's policy that the Company may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and interconnected VOIP) to which the customer already subscribes from the Company, without customer approval.

To the extent that the Company provides different categories of service, and a customer subscribes to more than one category of service offered by the Company, the Company may share CPNI among the Company's affiliated entities that provide a service offering to the customer. However, to the extent that the Company provides different categories of service, but a customer does not subscribe to more than one offering, the Company does not share CPNI with its affiliates, except by following the requirements described herein.

The Company does not use, disclose, or permit access to CPNI to market to a customer any service offerings that are within a category of service to which the subscriber does not already subscribe from the Company, unless the Company has customer approval to do so. The Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

Notwithstanding the forgoing, it is the Company's policy that the Company may use, disclose, or permit access to CPNI to protect the rights or property of the Company, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

C. Customer Approvals.

It is the Company's policy that the Company may obtain approval through written, oral or electronic methods. The Company acknowledges that it bears the burden of demonstrating that any oral approvals have been given in compliance with the Commission's rules. The Company honors all approvals or disapprovals to use, disclose, or permit access to a customer's CPNI until the customer revokes or limits such approval or disapproval. The Company maintains records of approval, regardless of the form of such approval, for at least one year.

Opt-Out and Opt-In Approval Processes. It is the Company's policy that it may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. It is the Company's policy that it may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services; and its joint venture partners and

independent contractors who do the same. It is the Company's policy that it may also permit such persons or entities to obtain access to such CPNI for such purposes. Except as provided herein, or as otherwise provided in Section 222 of the Communications Act of 1934, as amended, the Company only uses, discloses, or permits access to its customers' individually identifiable CPNI subject to opt-in approval.

D. Notice Required For Use Of Customer Proprietary Network Information. It is the Company's policy that prior to any solicitation for customer approval, notification is provided to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI. The Company maintains such records of notification, whether oral, written or electronic, for at least one year. It is the Company's policy that individual notice to customers is provided when soliciting approval to use, disclose, or permit access to customers' CPNI.

E. Notice Content Requirements. Company notices must comply with the following requirements:

1. Notices must provide sufficient information to enable the customer to make an informed decision as to whether to permit the Company to use, disclose, or permit access to, the customer's CPNI.

2. Notices must state that the customer has a right, and the Company has a duty, under federal law, to protect the confidentiality of CPNI.

3. Notices must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

4. Notices must advise the customer of the precise steps the customer must take in order to grant or deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes.

5. Notices must be comprehensible and must not be misleading.

6. To the extent that written Notices are provided, the Notices are clearly legible, use sufficiently large type, and are placed in an area so as to be readily apparent to a customer.

7. If any portion of a Notice is translated into another language, then all portions of the Notice must be translated into that language.

8. The Notice may state that the customer's approval to use CPNI may enhance the Company's ability to offer products and services tailored to the customer's needs. The Notice may also state that the Company may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

9. Notices may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

10. Notices must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from the Company is valid until the customer

SW

affirmatively revokes or limits such approval or denial.

11. The Company's solicitation for approval must be proximate to the Notice of a customer's CPNI rights.

F. Opt-Out Notice Requirements. It is the Company's policy that Notices to obtain opt-out approval be given only through electronic or written methods, and not by oral communication (except as provided with respect to one-time use of CPNI below).

The contents of any such notification must comply with the Notice Content Requirements described above.

It is the Company's policy to wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. This 30-day minimum period is calculated as follows: (1) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the Notice was sent; and (2) In the case of Notice by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed. It is the Company's policy to notify customers as to the applicable waiting period for a response before approval is assumed.

For those instances in which the Company uses the opt-out mechanism, the Company provides notices to applicable customers every two years.

For those instances in which the Company uses e-mail to provide opt-out notices, the Company follows the additional requirements in addition to the requirements generally applicable to notification:

(1) The Company must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

(2) The Company must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(3) Opt-out e-mail notices that are returned to the Company as undeliverable must be sent to the customer in another form before the Company considers the customer to have received notice;

(4) The subject line of the message must clearly and accurately identify the subject matter of the e-mail; and

(5) The Company makes available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week.

G. Opt-In Notice Requirements. It is the Company's policy that Notices to obtain opt-in approval be given though oral, written, or electronic methods. The contents of any such notification must comply with the Notice Content Requirements described above.

H. One-Time Use of CPNI Notice Requirements. The Company may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call. The Company requires that the contents of any such notification must comply

with the Notice Content Requirements described above, except that the Company may omit any of the following notice provisions if not relevant to the limited use for which the Company seeks CPNI:

(1) The requirement that the Company advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;

(2) The requirement that the Company advise customers that they may share CPNI with their affiliates or third-parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third-party;

(3) The requirement that the Company disclose the means by which a customer can deny or withdraw future access to CPNI, so long as explanation is given to customers that the scope of the approval the Company seeks is limited to one-time use; and

(4) The Company may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the Company clearly communicates that the customer can deny access to his CPNI for the call.

I. Safeguards Required for the Use of CPNI. It is the policy of the Company to train its personnel as to the circumstances under which CPNI may, and may not, be used or disclosed. In addition, the Company has established a written disciplinary process in instances where its personnel do not comply with established policies. It is the Company's policy to require that a record be maintained of its own and its affiliates' sales and marketing campaigns that use their customers' CPNI. The Company maintains a record of all instances where CPNI was disclosed or provided to other third-parties, or where third-parties were allowed to access such CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Such records are retained for a minimum of one year.

The Company has established a mandatory supervisory review process regarding compliance with CPNI rules for outbound marketing. Sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval. The Company's policies require that records pertaining to such carrier compliance be retained for a minimum period of one year.
In compliance with Section 64.2009(e), the Company will prepare a "compliance certificate" signed by an officer 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 47
C.F.R. § 64.2001 *et seq*. The certificate is to be accompanied by this statement and will be filed in EB Docket No. 06-36 annually on or before March 1, for data pertaining to the previous calendar year. This filing will 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.

It is the Company's policy to provide written notice to the FCC within five business days of any instance where the opt-out mechanisms do not work properly, such that a consumer's inability to opt-out is more than an anomaly. The written notice shall comply with 47 C.F.R. §64.2009(f).

J. Safeguards on the Disclosure of CPNI. It is the Company's policy to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The

Company will properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online access, or in-store visit, if applicable, as described herein.

(1) Methods of Accessing CPNI.

(a) Telephone Access to CPNI. It is the Company's policy to only disclose Call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the Company with a password, as described in Section (2), that is not prompted by the Company asking for readily available biographical information, or account information. If the customer does not provide a password, the Company will only disclose Call detail information by sending it to the customer's address of record, or, by calling the customer at the telephone number of record. If the customer is able to provide Call detail information to the Company during a customer-initiated call without the Company's assistance, then the Company may discuss the Call detail information provided by the customer.

(b) Online Access to CPNI. It is the Company's policy to authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in Section (2), that is not prompted by the Company asking for readily available biographical information, or account information.

(c) In Store Access to CPNI. It is the Company's policy that it may disclose CPNI to a customer who, at any retail location operated by the Company, first presents to the Company or its agent a valid photo ID matching the customer's account information.

(2) Password Procedures. To establish a password, the Company will authenticate the customer without the use of readily available biographical information, or account information. The Company may create a back-up customer authentication method in the event of lost or forgotten passwords, but such back-up customer authentication method will not prompt the customer for readily available biographical information or account information. If the customer cannot provide the correct password or correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(3) Notification of Account Changes. It is the Company's policy to notify customers immediately 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 notification may be through Company-originated voicemail or text message to the telephone number of records, or by mail to the address of record, and will not reveal the changed information or be sent to the new account information.

(4) Business Customer Exemption. It is the Company's policy that it may contractually be bound to other authentication regimes other than those described herein for services provided to business customers that have both a dedicated account representative and a contract that specifically addresses the Company's protection of CPNI.

K. Notification of CPNI Security Breaches.

(1) It is the Company's policy to notify law enforcement of a breach in its customers' CPNI as provided in this section. The Company will not notify its customers or disclose the breach publicly

until it has completed the process of notifying law enforcement pursuant to paragraph (2).

(2) As soon as practicable, and in no event later than seven (7) business days after reasonable determination of the breach, the Company will electronically notify the United States Secret Services (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility.

(a) Notwithstanding state law to the contrary, the Company shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI, except as provided in paragraphs (b) and (c).

(b) If the Company believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (a), in order to avoid immediate and irreparable harm, it will so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigation agency. The Company will cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(c) If the relevant investigating agency determines that public disclosure or notice to customer would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that the public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by the Company.

(3) Customer Notification. After the Company has notified law enforcement pursuant to paragraph (2), it will notify its customers of breach of those customers' CPNI.

(4) Recordkeeping. The Company will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (2), and notifications made to customers. The record will 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. The Company will maintain the record for a minimum of 2 years.