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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed February 25th, 2019
2. Name of company covered by this certification: Servicios Ampliados de Telefonos S. A. (SATEL) and Trilogy Dominicana, S. A.
3. Form 499 Filer ID: 822860
4. Name of signatory: Luis Bodega Belliard
5. Title of signatory: General Manager
6. Certification:

I, Luis Bodega Belliard, certify that I am an officer of both Servicios Ampliados de Telefonos S. A. (SATEL) and Trilogy Dominicana, S. A. (collectively, "Company") and, acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures, as summarized in the attached statement, that are adequate to ensure compliance with the Commission's customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the Commission's rules, 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 received any customer complaints in the past calendar year concerning unauthorized release of CPNI. Company has not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. §1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject the Company to enforcement actions.

Trilogy Dominicana, S. A. · Santo Domingo, República Dominicana ·

Luis Bodega Belliard
General Manager
Servicios Ampliados de Teléfonos S. A. and
Trilogy Dominicana, S. A.
Executed February 25, 2019

CPNI Compliance Policies of Trilogy Dominicana S.A. and Servicios Ampliados Telefonos, S. A.

Trilogy Dominicana S.A. ("TDR") and Servicios Ampliados de Telefonos, S. A. ("SATEL") (together, "Trilogy") submit the following to demonstrate that the companies are in compliance with Section 222 of the Communications Act and the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.* regarding the protection of Customer Proprietary Network Information ("CPNI") and carrier proprietary information. Trilogy's policy is administered by its CPNI Compliance Officer, Luis Bodega Beliard, General Manager.

In the United States, TDR is a long-distance connecting carrier that provides international service only to other telecommunications carriers, and not to end-user consumers. This policy applies only to TDR's sale of such wholesale services to its carrier customers inside the United States, and does not apply to TDR's services sold to end-user customers in the Dominican Republic, where it is based and conducts its main business operations.

For purposes of this policy, CPNI is (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a U.S. telecommunications service subscribed to by Trilogy's U.S. customers, and that is made available to Trilogy by such customers solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to U.S. telephone exchange service or telephone toll service received by Trilogy's U.S. customers.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

In accordance with Section 222(b) of the Act, 47 U.S.C. § 222(b), when Trilogy receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it only uses such information for such purpose. Trilogy does not use such information or any other CPNI for any marketing of any kind.

Trilogy may use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including activities to initiate, render, bill and collect for telecommunications services; to protect the rights or property of Trilogy, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Trilogy does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

A. Inbound Calls to Trilogy Requesting CPNI

Trilogy does not provide CPNI in response to requests from inbound callers. If Trilogy should decide to offer such access in the future, it will revise these policies to comply with the FCC's requirements for authentication of caller identity prior to disclosing CPNI, including Call Detail Information.

B. Online Access to CPNI

Trilogy does not offer customers the ability to access CPNI by means of online accounts. If Trilogy should decide to offer such access in the future, it will revise these policies to comply with the FCC's requirements for password protection of such accounts.

C. In-Person Disclosure of CPNI at Trilogy Offices

Trilogy does not provide access to CPNI to visitors at a retail office. If Trilogy should decide to offer such access in the future, it will revise these policies to require a visitor to show a valid, government-issued photo ID matching the customer's account information prior to revealing any CPNI.

D. Notice of Account Changes

When an address of record is created or changed, Trilogy will send a notice to a preexisting customer address of record notifying it of the change. This notice requirement does not apply when the customer initiates service. The notices will not reveal the changed information and will direct the customer to notify Trilogy immediately if it did not authorize the change. There are no passwords, customer response to a back-up means of authentication for lost or forgotten passwords, or online accounts associated with CPNI possessed by Trilogy.

E. Additional Safeguards

Above and beyond the specific FCC requirements, Trilogy will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The FCC's rules require carriers on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting." If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Trilogy's existing policies that would strengthen protection of CPNI, they should report such information immediately to Trilogy's CPNI Compliance Officer so that Trilogy may evaluate whether existing policies should be supplemented or changed.

Call detail information records are maintained in secure databases accessible only by a limited number of employees. To prevent unauthorized access to CPNI, Trilogy employees must use a login and password to obtain access to databases that include CPNI.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Trilogy employee that becomes aware of any breaches, suspected breaches or attempted breaches of CPNI must report such information immediately to the Trilogy CPNI Compliance Officer, and must not report or disclose such information by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Trilogy's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Trilogy's CPNI compliance policies are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when any person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Officer.

If a Trilogy employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Trilogy's CPNI Compliance Officer who will determine whether to report the incident to law enforcement and/or take other appropriate action. Trilogy's Compliance Officer will determine whether it is appropriate to update Trilogy's CPNI policies or training materials in light of any new information; the FCC's rules require Trilogy on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the Trilogy CPNI Compliance Officer shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. Trilogy's FRN number and password may be required to submit a report. If this link is not responsive, the Trilogy CPNI Compliance Officer will contact counsel or the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/eb/cpni) for instructions.

Except as provided below, Trilogy will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI. (A full business day does not count a business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure.

If Trilogy receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach. Trilogy will delay notification to customers or the public upon request of the FBI or USSS. If the Trilogy Compliance Officer believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Trilogy still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

IV. RECORD RETENTION

The CPNI Compliance Officer is responsible for assuring that Trilogy maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must 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.

Trilogy maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI.

Because Trilogy does not use CPNI for marketing or for any other purpose for which customer approval is required, it does not have any records regarding: supervisory review of marketing; sales and marketing campaigns that use CPNI; customers' "opt-out" approval or non-approval to use CPNI; or notifications to customers prior to any solicitation for customer approval to use or disclose CPNI.

Trilogy will maintain a record of any customer complaints related to their handling of CPNI, and records of Trilogy's handling of such complaints, for at least two years. The CPNI Compliance Officer will assure that all complaints are reviewed and that Trilogy considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Trilogy will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Trilogy has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Trilogy's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must 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.

V. TRAINING

All employees with access to CPNI of Trilogy's U.S. customers receive a summary of Trilogy's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission

not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, (ii) proprietary information Trilogy receives from another carrier for purposes of providing a telecommunications service may be used only for such purpose; and (iii) employees who knowingly facilitate the unauthorized disclosure of CPNI may be subject to criminal penalties.