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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2015 covering the prior calendar year 2014

1. Date filed: February 27, 2015
2. Name of company covered by this certification: PTGi International Carrier Services, Inc.
3. Form 499 Filer ID: 827965
4. Name of signatory: Craig Denson
5. Title of signatory: President

Certification:

I, certify that I am an officer of PTGi International Carrier Services, Inc. ("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 does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Company has therefore 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.

Craig Denson, President
PTGi International Carrier Services, Inc.
Executed February 27, 2015

PTGi International Carrier Services, Inc.
Statement of CPNI Compliance Procedures

PTGi International Carrier Services, Inc. ("PTGi ICS") has implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*.

CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

In accordance with Section 222(b) of the Communications Act, 47 U.S.C. § 222(b), when PTGi ICS receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it only uses such information for such purpose.

PTGi ICS 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 PTGi ICS, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to market services within the category or categories of services to which the customer already subscribes; to provide installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

PTGi ICS 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 PTGi ICS Requesting CPNI

PTGi ICS does not provide CPNI in response to requests from inbound callers. If PTGi ICS 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

PTGi ICS does not offer customers the ability to access CPNI by means of online accounts. If PTGi ICS 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 Company Offices

PTGi ICS does not provide access to CPNI to visitors at a retail office. If PTGi ICS 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, PTGi ICS 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 PTGi ICS 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 PTGi ICS.

E. Additional Safeguards

Above and beyond the specific FCC requirements, PTGi ICS 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 PTGi ICS's existing policies that would strengthen protection of CPNI, they should report such information immediately to the company's CPNI Compliance Manager so that PTGi ICS may evaluate whether existing policies should be supplemented or changed.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any PTGi ICS employee who becomes aware of any breaches, suspected breaches or attempted breaches of CPNI must report such information immediately to the CPNI Compliance Manager, 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 who fails to report such information will be subject to disciplinary action that may include termination.

It is PTGi ICS'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 PTGi ICS'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 Manager.

If a PTGi ICS 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 PTGi ICS's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action.

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the CPNI Compliance Manager shall electronically notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") by accessing the following link: http://www.cpnireporting.gov. PTGi ICS's FRN number and password may be required to submit a report.

Except as provided below, PTGi ICS will not notify customers or disclose a breach to the public until seven 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 PTGi ICS receives no response from law enforcement after the seventh full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach. PTGi ICS will delay notification to customers or the public upon request of the FBI or USSS. If the PTGi ICS Compliance Manager 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; PTGi ICS 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 Manager is responsible for assuring that PTGi ICS 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.

PTGi ICS 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 PTGi ICS 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.

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

PTGi ICS 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 PTGi ICS 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 Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how PTGi ICS'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 receive a summary of PTGi ICS'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 PTGi ICS 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.