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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009

1. Date filed: February 26, 2010
2. Name of company covered by this certification: Net 56, Inc.
3. Form 499 Filer ID: 826832
4. Name of signatory: Bruce L. Koch
5. Title of signatory: President
6. Certification:

I, Bruce L. Koch, certify that I am an officer of Net 56, 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 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.

Bruce L. Koch
President
Net 56, Inc.
Executed February 26, 2010

CPNI Compliance Policies of
Net 56, Inc.

The following summary describes the policies of Net 56, Inc. ("Company") that are designed 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

Company may use, disclose, or permit access to CPNI without customer approval 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 the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Company, 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 inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Except as provided above, Company does not use CPNI for marketing. In the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve the CPNI Compliance Manager. If such use is approved, Company shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

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

When Company receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, Company will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. 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 Company's existing policies that

would strengthen protection of CPNI, they should report such information immediately to Company's CPNI Compliance Manager so that Company may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to Company Requesting CPNI

Company does not disclose CPNI to an inbound caller unless the caller has been authenticated by correctly providing requested identifying information. The degree of authentication required may vary based upon the sensitivity of the information requested by the caller.

Notwithstanding the foregoing, Company does not disclose Call Detail Information (CDI) to inbound callers. CDI is a subset of CPNI that includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

If a caller requests CDI, Company may provide CDI by sending the information to an address of record for the account, but only if such address has been on file with Company for at least thirty (30) days; or in a call initiated by Company and placed to the customer's telephone number of record.

If an inbound caller is able to provide to a Company employee the telephone number called, when it was called, and, if applicable, the amount charged for the call, exactly as that information appears on the bill or online portal, then Company is permitted to discuss customer service pertaining to that call.

B. Online Accounts

Company does not provide online access to CPNI.

C. In-Person Disclosure of CPNI at Company Offices

Company may disclose a customer's CPNI to an authorized person visiting a Company office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

D. Notice of Account Changes

When an address of record is created or changed, Company will send a notice to customer's preexisting address of record. This notification is not required when the customer initiates service. The notice will not reveal the changed information and will direct the customer to notify Company immediately if they did not authorize the change.

E. Business Customer Exemption

Pursuant to 47 C.F.R. § 64.2010(g), the authentication requirements for disclosure of CPNI set forth in this section do not apply to the accounts of business customers that have both a dedicated account representative and a contract that specifically addresses the protection of CPNI.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Federal law imposes very specific requirements upon Company in the event that we become aware of any breach of customer CPNI. A breach includes any instance in which any person has intentionally gained access to, used, or disclosed a Company customer's CPNI beyond their authorization to do so. Any Company employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the Company CPNI Compliance Manager, and such information must not be reported or disclosed 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 Company'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 our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Company's CPNI compliance procedures 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 a 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 Company 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 Company's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. Company's Compliance Manager will determine whether it is appropriate to update Company's CPNI policies or training materials in light of any new information; the FCC's rules require Company 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 Company CPNI Compliance Manager 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. Company's FRN number and password may be required to

submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/eb/cpni) for instructions.

Company will not under any circumstances notify customers or disclose a breach to the public until seven (7) full business days have passed after notification to the USSS and the FBI except as provided below (a full business day does not count a business day on which the notice was provided).

If Company receives no response from law enforcement after the seventh (7th) full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach. Company will delay notification to customers or the public upon request of the FBI or USSS. If the Company CPNI 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 disclosure; Company still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

IV. RECORD RETENTION

The Company CPNI Compliance Manager is responsible for assuring that we maintain 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.

Company 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; supervisory review of marketing that proposes to use CPNI or to request customer approval to use or disclose CPNI; its sales and marketing campaigns that use its customers' CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, and the products and services offered as a part of the campaign; and records associated with customers' approval or non-approval to use CPNI, and of notification to customers prior to any solicitation for customer approval of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

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

Company 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 Company 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 Company'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 training in the appropriate handling and safeguard of customer information. Company requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel. All employees with access to CPNI receive information regarding Company'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, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. The CSR training emphasizes, among other points, that CSRs be cognizant that some unauthorized persons may have significant apparent familiarity with a customer's biographical and account information.