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: March 2, 2015
2. Name of company covered by this certification: Contact Communications, Inc.
3. Form 499 Filer ID: 824214
4. Name of signatory: Mitch Benson
5. Title of signatory: President

Certification:

I, Mitch Benson, certify that I am an officer of Contact Communications, 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 it 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.

Mitch Benson
President
Contact Communications, Inc.
Executed February 27, 2015

CONTACT COMMUNICATIONS

Customer Proprietary Network Information Compliance

Policy: We must properly authenticate a customer prior to disclosing account information or call detail information no matter the method of customer-initiated contact with our companies.

Policies and Procedures

Definitions

WyoPhone – The Company's voice service offered to the public for a price or fee. The service consists of both basic local and long-distance calling services and additional adjunct-to-basic services as determined by the customers, using Internet Protocol over broadband connections.

CPNI - Customer Proprietary Network Information

Call Detail Information - Anything associated with telephone calling history including telephone numbers dialed, length of calls, or any other WyoPhone usage information.

Primary Password - The primary password is the password found in the General tab of the customer's Platypus account, and is to be formed during initial customer account creation prior to actual WyoPhone service inception. Primary Passwords do not consist of any material portion of the WyoPhone customer's name, family names, account number, telephone number, street address, zip code, social security number, date of birth, or other biological or account information. Primary Passwords will also not consist of words easily-guessed strings of characters, such as consecutive or repeated digits.

Address of Record - The primary e-mail address found in the General tab of the customer's Platypus account or the Physical address found in the customer's Platypus account.

Account Information – Examples include biographical Information, primary account password a/k/a primary password, credit card and bank information, address detail, contact Information, invoice and payment history, account balance, account number, and WyoPhone service specs.

Employee Training

All employees must be trained on CPNI Policy and Procedures before any contact with WyoPhone customers is allowed. Employees 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 Company requires that each employee sign a statement once training has been completed that verifies the employee understands the policies and procedures.

Use, Disclosure and Access to CPNI

We may use, disclose, or permit access to CPNI only in our provision of the WyoPhone service from which such information is derived; for services necessary to, or used in, the provision of such WyoPhone service, including the publishing of directories; to initiate, render, bill and collect for WyoPhone services; to protect the rights or property of the company, or to protect users/customers or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

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

When we receive or obtain proprietary information from another carrier for purposes of providing a telecommunications service, we may use such information only for such purpose, and may not use such information for our own marketing efforts.

Marketing Practices

We may, without customer approval, use customer proprietary network information (CPNI) to market services to formerly known as adjunct-to-basic services to WyoPhone local telephone customers. Examples of these services include, but are not limited to, speed dialing, call forwarding, caller id, and call blocking. Any marketing effort to WyoPhone customers using CPNI must be approved by the President of the company and in accordance with Subpart U of Part 64, of Title 47 of the Code of Federal Regulations.

Telephone-initiated Customer Contact

At the beginning of the call, determine if the customer is a WyoPhone customer. If the customer is not a WyoPhone customer, please proceed as with all other Internet Service customers.

If the customer is a WyoPhone customer, then please ask for the customer's primary password before discussing any account information or call detail information. We must use the primary password, we cannot use any other information. We recommend the appropriate phrase of "*For security purposes, can you please tell me your primary account password?*"

Once the customer has given the correct password, the customer has been properly authenticated and you may discuss the entire account with that customer.

If the caller cannot provide the password, then you may respond using one of the following methods:

1. Send the password to the primary e-mail address of record on the account. We may not tell the caller which e-mail address we are sending the password to.
2. Call the customer back at the primary WyoPhone telephone number. If the customer answers, you may discuss the entire account. If the customer does not answer, you can leave the password on the voice mail.
3. Ask the customer what information they are trying to obtain, and send that information to the customer using the Address of Record, if that address has been on file with the company for at least thirty (30) days.. You may also communicate the information to the customer's WyoPhone voice mail.

Once you have authenticated the customer, the customer is free to make changes to their account. Some changes may generate a written or e-mail notice to the customer verifying that certain fields have been changed.

Any changes to a customer's account information must include notes or a ticket of the customer request and any action taken in response to that request.

Note: When transferring any WyoPhone customer to another department, you must advise your coworker if the WyoPhone customer has been properly authenticated.

Note for Business WyoPhone Customers: Authentication procedures are not as detailed herein. Employees are to treat Business WyoPhone customers just as they do standard Business customers of Wyoming.com Internet or Web services.

In-Person Contact

Determine if the customer is a WyoPhone customer. If the customer is not a WyoPhone customer, please proceed as with all other Internet Service customers.

If the customer is a WyoPhone customer, then please ask for the customer to present a valid, non-expired government-issued photo identification. Driver's license and passport will be the most common acceptable forms of identification. The address and name on the id must match the customer's account information.

Any changes to a customer's account information must include notes or a ticket of the customer request and any action taken in response to that request.

Note for Business WyoPhone Customers: Authentication procedures are not as detailed herein. Employees are to treat Business WyoPhone customers just as they do standard Business customers of Wyoming.com Internet or Web services.

On-line Access

The Company allows WyoPhone customers to access CPNI via online tools. The WyoPhone customer is required to enter their Primary Password prior to obtaining any account information. The customer's primary password must adhere to the definition as detailed within these CPNI Policies and Procedures. If the customer is unable to access CPNI online, then the customer is directed to contact the Company via telephone, and all policies and procedures outlined under *Telephone-initiated Customer Contact* are to be followed.

Notification of Account Changes

We must immediately notify a customer whenever a password, back-up password, or address of record is created or changed. This is not required at the time of service initiation. Notification may be by voicemail to the WyoPhone telephone number of record or by mail to the address of record and must not reveal the changed information or be sent to the new account information.

Customer Complaints or Breaches

All customer inquiries regarding unauthorized access or unauthorized changes to an account must be forwarded to the Department Supervisor/Manager. The Department Supervisor/Manager must report the specifics of the complaint to the Director of Public Policy. The Director of Public Policy is obligated to comply with the Notification procedures outlined below.

Notification of CPNI Security Breaches

We must notify law enforcement of any breaches of our customers' CPNI. A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. We cannot notify our customer(s) or disclose the breach publicly until we have completed the process of law enforcement notification as detailed herein:

1. As soon as practicable, and no later than seven business days, after reasonable determination of the breach, we must electronically notify the US Secret Service and FBI through the central reporting facility. The FCC link to the reporting facility is http://www.fcc.gov/eb/cpni.

   A) We cannot notify the customer(s) or disclose to the public until seven full business days (not counting a business day on which the notice was provided) have passed after notification to the US Secret Service and FBI except as provide in B or C;

   B) If we believe that there is "an extraordinarily urgent need" to notify any affected customer(s) sooner than allowed under A in order to avoid immediate and irreparable harm, we must indicate this in our notification and may proceed to immediately notify the affected customer(s) only after consultation with the relevant investigating agency. We must cooperate with the relevant investigating agency's request to minimize any adverse effects of any customer notification;

   C) If the relevant investigating agency determines that public disclosure or notice to customer(s) would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct us not to disclose or notify for initial period of up to thirty days. Such period may be extended by the agency in the judgment of the agency. If such direction is given, the agency shall notify us when it appears that the notice to customer(s) will no longer impede or compromise a criminal investigation or national security. The agency will provide any instructions or judgments in writing to us and such writings shall be logged on the same reporting facility that contains records of notifications filed by all carriers.

2. After we have notified law enforcement, as detailed in 1 above, we must notify the customer(s) of a breach of their CPNI.

3. We must maintain a record of any breaches of CPNI discovered, notifications of breaches made to law enforcement and customers. The records must include dates of discovery and notifications, a detailed description and circumstances of any breach. Records must be kept for a minimum of two years.

4. 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". Accordingly, if we determine that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, or if we become 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 our existing policies that would strengthen protection of

CPNI, we will review the information to determine whether to take appropriate action and/or supplement or revise these policies.

Additional CPNI Policies

The 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; of 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.

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

The Company will have an authorized corporate officer sign a compliance certificate on an annual basis stating that the officer has personal knowledge that we have established operating procedures that are adequate to ensure our compliance with the 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 the 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. Any confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.