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

EB Docket 06-36

Received & Inspected
FEB 2 0 2008
FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2007

Date filed: 02/15/08

DOCKET FILE COPY ORIGINAL

Name of company covered by this certification: Iowa Network Services, Inc.

Form 499 Filer ID: 804606

Name of signatory: Judith K. Langholz

Title of signatory: Vice-President of Product Support

I, Judith K. Langholz, 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 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.

Iowa Network Services, Inc. has not taken any actions (proceedings instituted or petitions at either state commissions, the court system, or at the Commission) against data brokers in the past year. Iowa Network Services, Inc. has no information with respect to the processes pretexters may use to attempt to access CPNI. The attached material describes the processes that Iowa Network Services, Inc. is taking to protect CPNI.

Iowa Network Services, Inc. has not received any customer complaints in the past year concerning the unauthorized release of CPNI. Iowa Network Services, Inc. is unaware of any instances of unauthorized access to CPNI, unauthorized disclosure of CPNI, 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.

Signed Judith K. Langholz

Iowa Network Services, Inc.

2007 Training Materials
New Employees and All Employee Annual Meetings

CPNI Rules

In 1999, the Federal Communications Commission (FCC) enacted rules protecting the personal customer information collected by local, long distance and wireless phone companies. The personal customer information includes phone numbers dialed by a customer, time calls are made, and the different services used by a customer. This type of personal information is referred to as Customer Proprietary Network Information (CPNI). Because of the CPNI rules, the FCC is empowered to investigate consumer complaints about unauthorized or unlawful disclosure of customer information, and can issue citations and propose fines.

Per the FCC rules, a phone company such as INS can release CPNI information only under the following circumstances:

- Over the Phone - If the customer calls into INS we can:
  - Mail the requested information to the address of record listed on the account,
  - Return the call to the phone number of record on the account to relay the requested information,
  - Or, if the customer is able to provide unprompted call detail information to you during a customer initiated call without your assistance, then you are permitted to discuss the call detail information provided by the customer.
- In Person - If the customer appears at your location and shows a valid photo ID that corroborates with your customer account information, you may disclose CPNI.

The only exception to the delivery of information to account holders is the category of businesses that have dedicated account reps. If they call in through their account rep, we can release the information on the call without a call back. If the business does not have an account rep, they will be treated as a consumer and all procedures above apply.

Access to INS CPNI information will be password protected and only available to those employees who need it for the completion of their job duties.

Disciplinary action for misuse of CPNI will be in accordance with company policy as stated in the INS Employee Manual.

Education

On an annual basis, INS will inform all employees of the rules and circumstances for disseminating CPNI. CPNI will also be discussed with new staff during new employee orientation.

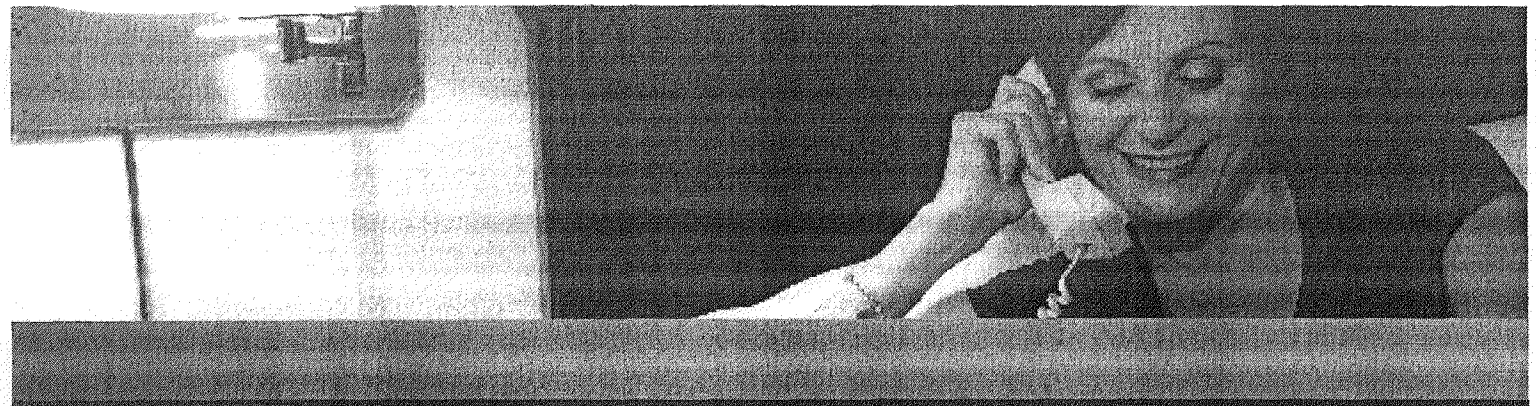
INS employees requiring access to CPNI data to fulfill job responsibilities will be provided initial and ongoing training on the proper access and usage of personal customer information. These individuals will also be trained on their responsibilities in protecting CPNI.

INS does not use CPNI for sales or marketing purposes.

INS does not disclose CPNI data outside the company except when required by a lawful subpoena, for purposes of billing and collection, or when necessary to protect the rights or property of the company or its customers.

IOWA NETWORK SERVICES

Policies and Procedures Handbook



INS Connects

Issued: March 14, 2003
Revised: August 21, 2007

STANDARDS OF CONDUCT

Confidentiality

The protection of confidential, sensitive and proprietary business information and trade secrets is vital to the interests and the success of INS. Many of our employees need access to confidential company and customer information and records in order to do their jobs. While an open climate of information sharing is most often desirable, there is a need to safeguard the security of information that could be detrimental to the company or our customers and information that could be advantageous to our competitors. Such confidential information includes, but is not limited to, the following examples:

- Computer programs and code
- Electronic data (files/programs)
- Personnel and compensation data
- Customer and mailing lists
- Financial reports or data
- Computer printouts
- Program documentation
- Company manuals
- Customer business information, methods
- Correspondence
- Marketing strategies
- Pending projects and proposals

In addition to the items listed above, confidential information also includes any other information that a prudent person could reasonably believe to be confidential.

Employees who improperly use or disclose trade secrets, confidential business information or information concerning a customer will be subject to disciplinary action, up to and including termination of employment, even if they do not actually benefit from the disclosed information. Such employees may also be subject to legal action.

Customer Proprietary Network Information

Customer Proprietary Network Information (CPNI) includes the type, technical arrangement, quantity, destination, and amount of use of telecommunications services and related billing for these services for a specified individual customer.

Operating Procedures for Compliance with CPNI Regulations

- Procedures/systems requiring customer verification prior to disclosure of CPNI. The verification process is to ensure the person requesting access to CPNI is the customer.
- Limited password access to CPNI data by Company personnel to ensure only trained and authorized individuals have the ability to see this data.
- Education of company personnel regarding the use of CPNI data.
- Disciplinary procedures regarding inappropriate use of CPNI data.
- Company policy is not to use CPNI data in sales and marketing campaigns.
- Company policy is non-disclosure of any CPNI data outside of the company, except when required by a lawful subpoena, for purposes of billing and collection, and when necessary to protect the rights or property of the company or its customers.