IOWA NETWORK SERVICES

4201 Corporate Drive
West Des Moines, IA
50266-5906

P 800.469.4000
F 515.830.0123

Received & Inspected

FEB 21 2012

FCC Mail Room

February 15, 2012

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW - Suite TW-A325
Washington, DC 20554-0004

Re: EB Docket No. 06-36, Certification of CPNI Filing

Dear Ms. Dortch:

Enclosed in this mailing please find the required 2011 CPNI certification and support documents for Iowa Network Services, Inc.

If you have any questions regarding this filing, please feel free to contact me.

Sincerely,

Judith K. Langholz

Judith K. Langholz, Vice-President of Product Support

cc: Best Copy and Printing, Inc., Portals II, 445 12th Street, SW, Suite CY-B402, Washington, DC 20554-0004

No. of Copies rec'd 0+4
List ABCDE

Received & Inspected

FEB 21 2012

FCC Mail Room

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2011

Date filed:	**02/15/12**
Name of company(s) covered by this certification:	**Iowa Network Services, Inc.**
Form 499 Filer ID:	**804606**
Name of signatory:	**Judith K. Langholz**
Title of signatory:	**Vice President – 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 (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 taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

There have been no CPNI attempted access attempts of which I am aware.

The company has not received any customer complaints in the past year concerning the unauthorized release or unauthorized disclosure of CPNI.

The Company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed: Judith K. Langholz

Judith K. Langholz Vice President – Product Support

Attachments: Accompanying Statements explaining CPNI procedures
A section of the INS Policies and Procedures Handbook
2011 Training Materials

IOWA NETWORK SERVICES

4201 Corporate Drive
West Des Moines, IA
50266-5906

P 800.469.4000
F 515.830.0123

2011 INS Report of Identify Theft
Submitted to the INS Board for Approval *09/20/2011*

As the INS Red Flag Coordinator and reporter of activities related to Identify Theft prevention, I have reviewed the procedures in place and operational activities of the period 09-17-2010 to 09-09-2011. My findings are summarized below:

- Notification:

Human resources has the Identify Theft Program and Manual available on the INS Intranet for all personnel to access.

- Training:

Each INS VP with employees having responsibilities and access to customer financial information has discussed the topic of Identify Theft, INS procedures and the related action steps with their staff.
Each INS VP with employees having responsibilities and access to customer financial information has held individual employee training in this period that included training on the INS Red Flag procedures and action steps, and has also maintained an employee training signature page.

- Occurrences:

All INS VPs have been polled regarding known instances of Identify Theft or compromised data in this period.
For this period INS VPs report that there are no known instances of Identify Theft or compromised data.

- Updating:

In the event of any compromise of data or identity theft the INS Board would review these instances during its annual review of Company operations and Budget process.

Submitted this 9th day of September, 2011

Judith K. Langholz
Vice President Product Support

INS

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.

* Employees in Finance and Customer Care with access to customer's personal financial data are required to adhere to Red Flag Rules. A separate document outlining these regulations titled *Red Flag Rules* is located on the Lawson Portal.

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.

IOWA NETWORK SERVICES

4201 Corporate Drive
West Des Moines, IA
50266-5906

P 800.469.4000
F 515.830.0123

Iowa Network Services, Inc.

2011 Training Materials
New Employees and All Employee Annual Meetings

IOWA NETWORK SERVICES

4201 Corporate Drive
West Des Moines, IA
50266-5906

P 800.469.4000
F 515.830.0123

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.

IOWA NETWORK SERVICES

4201 Corporate Drive
West Des Moines, IA
50266-5906

P 800.469.4000
F 515.830.0123

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

4201 Corporate Drive
West Des Moines, IA
50266-5906

P 800.469.4000
F 515.830.0123

INS CPNI CERTIFICATION TRAINING

I am aware that my job duties may include dealing with customers and their CPNI and/or the issue of identity theft. I have participated in a training session that covers my responsibilities and understand the role that I play.

NAME	DEPARTMENT	DATE OF TRAINING

The people listed above have received the training information regarding CPNI regulations.