

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

EB Docket 06-36

Annual certification for: 2007

Date filed: February 29, 2008

Name of companies covered by this certification: Insight Midwest Holdings, LLC; Insight Phone of Kentucky, LLC; Insight Phone of Indiana, LLC; Insight Phone of Ohio, LLC; Insight Phone of Illinois, LLC; Insight Communications Midwest, LLC; and Insight Kentucky Partners II, L.P.

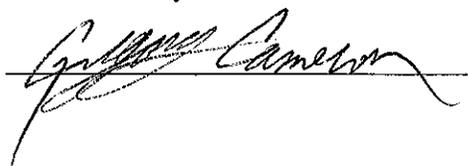
Form 499 Filer ID: Insight Midwest Holdings, LLC - 825350; Insight Phone of Kentucky, LLC - 823166; Insight Phone of Indiana, LLC - 823164; Insight Phone of Ohio, LLC - 825351; Insight Phone of Illinois, LLC - 825562; Insight Communications Midwest, LLC - 825419; and Insight Kentucky Partners II, L.P - 826535.

Name of signatory: Gregory Cameron

Title of signatory: VP of Telecom Legal Affairs

I, Gregory Cameron, VP of Telecom Legal Affairs, certify that I am an officer of the company(ies) 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. 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. The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, 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



Compliance Statement

The following statement is provided pursuant to 47 U.S.C. §64.2009(e) to explain how the operating procedures of Insight Midwest Holdings, LLC, on behalf of itself and its affiliates listed on the CPNI Certification ("Insight") ensure compliance with the applicable rules affecting use of customer proprietary network information.

Insight's policies and procedures to meet the CPNI guidelines include:

Company-Wide Training:

- All employees and contractors with access to CPNI must go through CPNI training prior to accessing CPNI. Insight tracks employee compliance and requires all contractors to certify that their employees shall comply with all CPNI requirements.
- All new hires who use CPNI information for sales or marketing activities must go through the training course prior to accessing or using CPNI.
- All employees with access to CPNI are required to review CPNI training on an annual basis and following any significant changes in the law occur. Insight's legal department will notify individual Company markets and departments of any changes in the law that necessitates additional CPNI training.
- Managers receive customer confidentiality training on an annual basis.
- Managers monitor and coach employees on maintaining customer confidentiality.

Account Protections:

- Documentation of customer CPNI permission status is maintained in the individual customer's account file in the Insight billing system.
- Insight does not permit Customers to establish account passwords and, therefore, does not provide customer CPNI information, including call detail information, during a customer initiated telephone contact or permit customers to access call detail information online. If a customer requests CPNI information during a customer initiated telephone contact, the call will be escalated to a customer service manager who will call the customer back at the account telephone number and then provide the information requested.
- Customers who request access in person at an Insight location are required to present valid photo identification.

- Insight notifies customers immediately by mail to the address of record whenever an address of record is changed. The notification does not reveal the changed information.

Marketing Safeguards:

- The Insight Marketing Director approves all direct marketing to ensure compliance with the CPNI rules.
- The Insight Marketing Department does not use customer CPNI for sales and marketing purposes and has safeguards to prevent cross-product information sharing that would be in violation of CPNI rules.
- The Insight Marketing Department does not sell customer lists to outside sources.
- If, in the future, Insight does use CPNI for sales and/or marketing campaigns, it shall maintain records of all sales and marketing campaigns that use CPNI.
- Insight maintains records of all instances, if any, where CPNI is disclosed or provided to third parties, or where third parties are permitted access to CPNI. These records are maintained for a minimum of one year.
- Insight has a supervisory review process to ensure compliance with CPNI restrictions when conducting outbound marketing.

Customer Service Safeguards:

- The Insight training department provides CPNI training to all customer service new hires and to all applicable department employees on an annual basis.
- Customers must verify their personal account information before an employee can provide comments or take requests for any changes to an account. At a minimum, customers must provide their name, address and verifiable account information.
- Detailed customer calling records, which are considered particularly confidential, are accessible only by employees or agents with a need to know and are provided to customers only during an Insight outbound call to the customer at the telephone number of record or, in the case of a request made in person at an Insight retail location, after the customer present valid identification.
- Customer service representative interactions with customers are monitored, and the monitoring includes evaluation of compliance with privacy requirements.

Notification of CPNI Security Breaches

- Insight shall notify law enforcement of all breaches of its customers' CPNI pursuant to the procedures and timeframes described in Section 64.2011 of the FCC's rules.
- Insight shall notify customers of all breaches of their CPNI pursuant to the procedures and timeframes described in Section 64.2011 of the FCC's rules.

Accountability:

- Persons who fail to comply with Insight's CPNI procedures are subject to a disciplinary process that can include dismissal.
- Compliance with CPNI safeguards is part of each applicable employee annual performance evaluation. Compliance can affect employees' continued employment.

Recordkeeping

- Insight's telephone CPNI policy is maintained by the Insight Legal Department and is posted on Insight's internal policy database for training and employee policy review purposes.
- Insight shall maintain for 2 years (minimum) a record of all discovered breaches of CPNI and breach notifications to law enforcement and customers. The records include, to the extent possible, the dates of discovery and notification, a detailed description of the CPNI that was breached, and the circumstances of the breach.

Actions Taken Against Data Brokers in the Past Year

None.

Summary of CPNI Complaints Received in Past Year

No CPNI complaints received in the past year.