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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: 3/1/10

Name of company covered by this certification: Flowroute, LLC

Form 499 Filer ID: 827496

Name of signatory: Sean Hsieh

Title of signatory: Chief Strategy Officer

I, Sean Hsieh, 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.

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. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps companies are taking to protect CPNI.

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 _____

Sean Hsieh
Chief Strategy Officer

Flowroute, LLC
CPNI Compliance Statement

Flowroute, LLC, ("Company") does not use, disclose or permit access to, Customer Proprietary Network Information ("CPNI") except as permitted under 47 U.S.C. § 222(d), except as otherwise required by law pursuant to 47 U.S.C. § 222(c)(1) or except as permitted under 47 U.S.C. §§ 222(c)(1)(A) and 222(c)(1)(B).

A. Definitions

The terms used in this Statement have the same meaning as set forth in 47 C.F.R. § 64.2003.

B. Use of CPNI

(1) The Company may, if applicable, use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes from the Company, without customer approval. If the Company provides different categories of service, and a customer subscribes to more than one category of service offered by the Company, the Company is permitted to share CPNI among its affiliated entities that provide a service offering to the customer.

(2) The Company may, if applicable, use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(3) The Company, as a provider of interconnected VoIP services, as that term is defined in 47 C.F.R. § 9.3, may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

(4) The Company does not use, disclose, or permit access to CPNI to market service offerings to a customer that require opt-in or opt-out consent of a customer under 47 C.F.R. § 64.2001 *et seq*.

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

(6) Notwithstanding the forgoing: It is the Company's policy that the Company may use, disclose, or permit access to CPNI to protect the rights or property of the Company, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

C. Safeguards Required for the Use of CPNI

(1) It is the policy of the Company to train its personnel as to the circumstances under which CPNI may, and may not, be used or disclosed. In addition, the Company has established a written disciplinary process in instances where its personnel do not comply with established policies.

(2) In compliance with Section 64.2009(e), the Company will prepare a "compliance certificate" signed by an officer on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with 47 C.F.R. § 64.2001 *et seq*. The certificate is to be accompanied by this statement and will be filed in EB Docket No. 06-36 annually on March 1, for data pertaining to the previous calendar year. This filing will 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.

D. Safeguards on the Disclosure of CPNI

It is the Company's policy to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The Company will properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online access, or in-store visit, if applicable, as described herein.

(1) *Methods of Accessing CPNI.*

(a) *Telephone Access to CPNI.* It is the Company's policy to only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the Company with a technical user prefix and interconnection password, as described in Section (2), that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer is able to provide call detail information to the Company during a customer-initiated call without the Company's assistance, then the Company may discuss the call detail information provided by the customer.

(b) *Online Access to CPNI.* It is the Company's policy to authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in Section (2), that is not prompted by the Company asking for readily available biographical information, or account information.

(c) *In-store Access to CPNI.* If applicable, it is the Company's policy that it may disclose CPNI to a customer who, at the Company's retail location, first presents to the Company or its agent a valid photo ID matching the customer's account information.

(2) *Password Procedures.*

To establish a password, the Company will authenticate the customer without the use of readily available biographical information, or account information. The Company may create a back-up customer authentication method in the event of lost or forgotten passwords, but such back-up customer authentication method will not prompt the customer for readily available biographical information or account information. If the customer cannot provide the correct password or correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(3) *Notification of Account Changes.*

The Company will notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a Company-originated voicemail or text message to the 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.

(4) *Business Customer Exemption.*

The Company may bind itself contractually to authentication regimes other than those described in this Section D for services it provides to its business customers that have both a dedicated account representative and a contract that specifically addresses the Company's protection of CPNI.

E. Notification of CPNI Security Breaches

(1) It is the Company's policy to notify law enforcement of a breach in its customers' CPNI as provided in this section. The Company will not notify its customers or disclose the breach publicly until it has completed the process of notifying law enforcement pursuant to paragraph (2).

(2) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the Company will electronically notify the United States Secret Services (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility.

(a) Notwithstanding state law to the contrary, the Company will not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI, except as provided in paragraphs (b) and (c).

(b) If the Company believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (a), in

order to avoid immediate and irreparable harm, it will so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigation agency. The Company will cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(c) If the relevant investigating agency determines that public disclosure or notice to customer would impede or compromise an ongoing or potential criminal investigation or national security, the Company will comply with such agency's written directives, including directives not to so disclose or notify for an initial period of up to 30 days, and extended periods as reasonably necessary in the judgment of the agency.

(3) After the Company has completed the process of notifying law enforcement pursuant to paragraph (2), it will notify its customers of a breach of those customers' CPNI.

(4) *Recordkeeping*. The Company will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (2), and notifications made to customers. The record will 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. The Company will maintain the record for a minimum of 2 years.