

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

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2010

Names of Companies covered by this certification:

Broadvox, LLC (Form 499 Filer ID 826005)
InfoTelis Corporation (Form 499 Filer ID 826004)
BroadvoxGo!, LLC (Form 499 Filer ID 827091)
Brivia Acquisition, LLC (Form 499 Filer ID 828028)
Origination Technologies, LLC (Form 499 Filer ID 827641)

Name of Signatory: Pete Sandrev

Title of Signatory: Vice President, Broadvox, LLC
President, InfoTelis Corporation
Vice President, BroadvoxGo!
Vice President, Brivia Acquisition, LLC
Vice President, Origination Technologies, LLC

Date: February 21, 2010

I, Pete Sandrev, certify that I am an officer of Broadvox, LLC, InfoTelis Corporation, BroadvoxGo!, LLC, Brivia Acquisition, LLC, and Origination Technologies, LLC (collectively "the Companies") and acting as an agent on behalf of each company, that I have personal knowledge that it has operating procedures and policies in place that are designed to ensure compliance with the Federal Communication Commission's ("Commission") CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how each company's procedures are designed to maintain compliance with the Commission's CPNI rules. The attached statement applies to all five companies.

The companies did not take any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers during the 2010 calendar year. The companies did not receive any complaints during 2010 concerning the unauthorized release of CPNI.

BroadvoxGo does not believe that any breaches of security or CPNI rule violations have occurred, but submits the following information out of an abundance of caution. In approximately October, 2010, one of BroadvoxGo!'s customers informed BroadvoxGo! that it was sending the customer's bill to the wrong e-mail address. Apparently, the customer had

provided a new e-mail address to which bills should be sent, but that notification of new billing address was not received and processed by the appropriate individuals. Indeed, the customer sent it to specific individuals rather than to the customer service department or to the address set forth in the contract for all notices. It appears that several invoices did, in fact, go to an incorrect e-mail address. That e-mail address belonged to a former employee of the customer, which former employee had set up the account when he had been employed by the customer. BroadvoxGo! believes several invoices went to the improper party. The customer and BroadvoxGo! have reached an agreement concerning the misdirected invoices. The customer has agreed that BroadvoxGo! is not liable concerning same.

Each company has taken measures to protect against attempts to gain unauthorized access to CPNI. The companies have not discovered any information about the processes that pretexters are using to attempt to gain access to CPNI other than the information that already is contained publicly in this docket. As mentioned in Attachment A, the companies have implemented CPNI safeguards, including, without limitation, maintaining customer verification processes, and applying role-based authorization (limiting employees with access to data on a need-to-know basis).

Signature:

A handwritten signature in black ink, appearing to read "P. G. Gault", written over a horizontal line.

February 23, 2010

ATTACHMENT A
BROADVOX, LLC
INFOTELIS CORPORATION
BROADVOXGO!, LLC
BRIVIA ACQUISITION, LLC
ORINATION TECHNOLOGIES, LLC

STATEMENT OF CPNI OPERATING PROCEDURES

Broadvox, LLC, InfoTelis Corporation, BroadvoxGo!, LLC, Brivia Acquisition, LLC, and Origination Technologies, LLC (collectively "the Companies") have established policies and procedures that are designed to ensure they are in compliance with the Federal Communications Commission's ("Commission") rules regarding the use, disclosure, and access to CPNI. The Companies provide this statement pursuant to Section 64.0009(e) of the Commission rules, 47 C.F.R. § 64.0009(e), to summarize those procedures and policies. As part of these processes and procedures, the Companies have appointed a compliance officer, responsible for overseeing the company's compliance with the FCC's CPNI rules.

PERMISSIBLE USES OF CPNI

The Companies are committed to protecting its customers' privacy, and they limit their employees access to and use of CPNI. The Companies may use CPNI for the following purposes: (1) to initiate, provide, and bill and collect for the telecommunications services from which such information is derived; (2) to provide the services necessary to, or used in, the provision of the VoIP services the Companies provide, including in the publishing of directories; (3) to market services to the Companies' customers within the category of service to which the customer subscribes; and (4) to protect the Companies' rights and property, or to protect the Companies' customers and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, our services. We also may use CPNI to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if the customer initiated the call and approves of the use of such information to provide services.

The Companies have implemented protections to protect against unauthorized disclosure or access to CPNI in the limited instances where it is required to share or disclose CPNI with third parties, such as for billing and collection.

USE OF CPNI FOR MARKETING PURPOSES

The Companies do not use CPNI to market products and services to customers. Therefore, it is not subject to the customer notice requirements. If the Companies subsequently seek to use CPNI to market products and services for such purposes, then they will provide

advance customer notification and seek appropriate approval from its customers before doing so. The Companies do not share CPNI with joint venture partners or independent contractors for marketing purposes.

EMPLOYEE TRAINING/DISCIPLINARY PROCESS:

The Companies train their personnel as to what information is classified as CPNI and as to when they are and are not authorized to use CPNI. The Companies have an express disciplinary process for the misuse of CPNI, which includes the potential for termination.

SAFEGUARDS

Employees must follow specific procedures to authenticate its customers. The Companies authenticate all in-coming calls. The Companies also have implemented password protection for online account access. All online accounts are password protected, and The Companies establish those passwords without the use of readily available biographical information or account information. The Companies have also implemented procedures to address lost or stolen passwords (such as challenge questions) that do not rely on the use of readily available biographical or account information. The Companies do not have any retail locations.

All the Companies' employees are prohibited from disclosing call detail information during an in-bound call. Employees only are permitted to disclose call detail information to the email address of record. The Companies have procedures in place to ensure that the email address has been in place for at least thirty days. The Companies also limit internal disclosure of CPNI to those employees with a need-to-know.

The Companies have implemented network security measures, including, but not limited to, the use of encryption. Under the Companies' compliance program, employees are required to ensure that customer data is protected from pretexting and other unauthorized access. The Companies' employees are required to notify the Compliance Officer of any suspected attempts to gain access to a customer's CPNI whether through pretexting or otherwise.

The Companies have implemented procedures for notifying customers of certain account changes, including, changes in online passwords, changes to online accounts, changes to a back-up means of authentication, and changes to the address of record.

The Companies have procedures in place for responding to requests for information from law enforcement personnel or from any person other than the customer.

DATA SECURITY BREACHES

The Companies will notify the United States Secret Service and the Federal Bureau of Investigation through the FCC's specifically designated portal (www.fcc.gov/eb/cpni) within seven days of the reasonable discovery of a data breach. In accordance with the FCC's rules, the Companies will notify affected customers of the breach, unless requested to withhold disclosure by the USSS or the FBI. The Companies' Compliance Officer will maintain a record

in accordance with section 64.2011(d) of any breaches discovered, notifications made to law enforcement, and notifications made to customers for at least two years.

CUSTOMER COMPLAINTS

The Companies track customer complaints they receive concerning the unauthorized use, disclosure, or access to CPNI. If we receive complaints regarding CPNI, we will break them down by category, and provide a summary of the complaints in the annual certification that we provide to the Commission.

NOTIFICATION OF ACCOUNT CHANGES

The Companies notify their customers immediately, via email, of certain account changes including any changes in the customer's online password, a change in the customer's address of record, a change in the customer's online account, and a change of the back-up means of authentication for lost or stolen passwords.