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

Annual 64.2009(e) CPNI Certification for Calendar Year 2014

Date filed: February 18, 2015

Name of company covered by this certification	FRN:
Birch Communications, Inc.	0005044375
Birch Communications of Virginia, Inc.	0020212890
Birch Communications of the Northeast, Inc.	0020152054
Birch Telecom of Missouri, Inc.	0003732294
Birch Telecom of Kansas, Inc.	0003732260
Birch Telecom of Oklahoma, Inc.	0003732328
Birch Telecom of Texas Ltd., L.L.P.	0003732336
Birch Telecom of the Great Lakes, Inc.	0005072780
Birch Telecom of the West, Inc.	0008159725
Birch Telecom of the South, Inc.	0004319299
Ionex Communications, Inc.	0005027453
Ionex Communications North, Inc.	0005027305
Ionex Communications South, Inc.	0005027420
Birch Communications of Kentucky, LLC	0022823819
Cbeyond Communications, LLC	0003759602

Name of signatory: Christopher Bunce

Title of signatory: Sr. Vice President

I, Christopher Bunce, 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 / Christopher Bunce /
Christopher Bunce, Sr. Vice President

Safeguarding Customer Proprietary Network Information
Birch Communications, Inc. Policy and Employee Guidelines

***Policy Statement*:** It is the policy of Birch Communications, Inc. and its subsidiaries ("Birch") to protect and maintain the confidentiality of customer proprietary network information as required by federal law. The company has a duty under federal law to protect the confidentiality of customer information and relies on its employees to fulfill that duty. Customer proprietary network information will be used or disclosed by Birch employees only in accord with applicable federal regulations and Birch procedures as described below.

***Types of customer information protected*:** During the course of a customer's relationship with Birch, the company will come into possession of information about the customer's use of the company's services. Federal law specifically protects customer information that relates to the quantity, technical configuration, type, destination, location, and amount of use of the customer's service, as well as any telephone service information contained in the customer's bill.[1/] Such information may include, for example, the phone numbers called by a customer, the length of the calls, and records of additional services purchased by the customer, such as voice mail.

***Restrictions on use and disclosure of customer information*:** Customer information may not be used by or disclosed to anyone outside of Birch without the customer's permission. Within Birch, customer information may not be used to market services in any category of services to which the customer does not currently subscribe, unless the customer has given permission. Categories of service for purposes of this restriction are local exchange service, long-distance service, and wireless service.

***Types of Customer Permission Required*:** Different types of customer permission are required for different types of customer information use or disclosure. Upon written request from the customer, the customer's information may be disclosed to any person designated by the customer. Customers seeking to access their customer information on-line must produce a password previously set by the customer.

Customers seeking to access their information by telephone must produce a password/access code[2/] to obtain release over the phone of call detail information.[3/] A customer who has lost, forgotten, or otherwise cannot locate his or her password may be authenticated by correctly answering one or more questions established with Birch at the time the password was

---

1/ These types of information have been termed "customer proprietary network information" or "CPNI" by the Federal Communications Commission.

2/ The requirement to produce a password does not apply to business customers where: (a) the customer's contract is serviced by a dedicated account representative as the primary contact; (b) the contract specifically addresses the protection of customer information; and (c) the business customer is not required to go through a call center to reach a customer service representative.

3/ Call detail information is any information that pertains to the transmission of specific telephone calls including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed and the time, location, or duration of the call.

set up. Customer information (other than call detail) may be given to the customer over the phone without a password once the customer satisfies the Birch employee of his or her identity. Customers may, over the phone without producing a password, request that Birch send call detail information to the customer's postal or e-mail address of record or request that Birch call the customer's telephone number of record with the requested call detail.

Customer permission required for Birch use of customer information in various types of marketing is described further below.

***Exceptions to use and disclosure restrictions*:** The law allows Birch to use or disclose customer information without permission for the following purposes:

1. to provide services (including installation, maintenance, repair, and billing for services) in any category of services to which the customer subscribes;
2. to market services (including marketing upgrades to basic service) in any category of services to which the customer already subscribes;
3. to publish directories or allow other parties to publish directories;[4/]
4. to protect Birch, its customers, or other parties against fraudulent, abusive or unlawful use of services; or
5. to respond to a legal demand for the information (*e.g.*, a subpoena or court order).

Supervisors may authorize employee use of customer information for purposes #1 and #2, above. Use of customer information for purpose #2 must follow guidelines described below. Use or disclosure of customer information for purpose #3 may only be undertaken with the authorization and guidance of the Birch General Counsel. Supervisors faced with a situation described in purposes #4 and #5 should consult with the Security and Fraud Department before using or disclosing any customer information. Questions about any of these situations, or demands for use of customer information other than those described above should be directed to Tara Jackson at (816) 300-1677 or Chris Bunce at (816) 300-3322.

***Customer permission to use or disclose customer information for marketing campaigns*:** Birch may seek permission from customers to use their customer information in marketing campaigns for other categories of services than those to which the customer currently subscribes. Once customer permission has been obtained, customer information may be used by Birch to market communications-related services to that customer in any category of services.[5/] Customer permission does not allow the use or disclosure of customer information for any other purpose, including the marketing of non-communications-related services.[6/]

4/ Only names, telephone numbers, addresses, and advertising classification (if any) may be used or disclosed for this purpose. If a customer has requested an unlisted number, information may not be disclosed for directory publication purposes.

5/ The "opt-out" permission system used by Birch does not extend to use of customer information for marketing by joint venture partners or independent contractors.

6/ Except, of course, for those purposes for which customer permission is not required, as described above.

***Records of customer permission of use or disclosure of customer information for marketing*:** Customer records will be clearly marked as to whether permission for use or disclosure of customer information for marketing of communications related services has been granted. For customers whose records are not marked showing permission has been granted, Birch employees must assume permission has not been granted.

***Approval and Recordkeeping for Use of Customer Information in a Marketing Campaign*:** Before a supervisor may authorize employees to use customer information for marketing purposes, the proposed use of customer information must be reviewed and approved by the General Counsel or a member of the Legal and Regulatory Department to assure the proposed use conforms with this policy and applicable federal regulations.[7/] Records of these reviews, including a description of the campaign, the specific customer information used in the campaign, and what products and services were offered as part of the campaign, will be maintained by the Product/Marketing Department.

Upon completion of a marketing campaign that uses customer information, or at regular intervals during the campaign, the appropriate leader of the Product/Marketing Department will review the campaign to ensure the use of customer information is in accord with this policy. Copies of such evaluations will be maintained by the marketing department for maintenance in the record of the campaign.

***Employee Training*:** As part of initial orientation and training, all new employees will be provided training on Birch policies and procedures with regard to protection and appropriate access and use of customer information. Training specific to each marketing campaign will be provided to employees at the initiation of any marketing campaign that uses customer information.

***Required Notifications and Annual Certification*:** To allow a customer to verify any change was intentional, Birch's Customer Service Center will notify a customer immediately, through telephone call to the customer's number of record or mail to the customer's address of record,[8/] of any changes to the customer's on-line account, address of record, password, or authentication questions established when the password was set up.

In any instance where a security breach results in customer information being disclosed to a third party without the customer's authorization, the employee discovering the breach must immediately notify the appropriate supervisor, who will notify a member of the Birch Legal and Regulatory Department. The Legal and Regulatory Department will, no later than seven days after determination of the breach, notify law enforcement through an online central

---

7/ This requirement applies both to campaigns to market services in categories to which the customer already subscribes (i.e., campaigns that do not require customer permission) and to campaigns using opt-out permission to market communications-related services or communications services in categories to which the customer does not already subscribe.

8/ A customer's address of record may be any address, either postal or electronic (*e.g.*, e-mail), that has been associated with the customer's account for at least 30 days. The telephone number of record must be a number in Birch's records associated with the customer account prior to any account changes that prompt the notification call.

reporting facility maintained by the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"). Unless instructed otherwise by law enforcement, Birch will notify the customer of the breach seven days after reporting it to the USSS and FBI.

In any instance where the opt-out mechanism for customer approval for use of customer information in marketing does not work properly to such a degree that customers' inability to opt out is more than an anomaly, the appropriate supervisor must immediately notify the Legal and Regulatory Department, which will provide the required notification to the Federal Communications Commission.

A member of the Birch senior management team will, by March 1st of each year, execute the required certification of Birch's compliance with customer information protection regulations along with the required report of actions taken against data brokers attempting to obtain customer information and summary of consumer complaints of unauthorized release of customer information during the previous calendar year.

***Penalties for misuse or inappropriate disclosure of customer information; reporting misuse*:** Misuse or inappropriate disclosure of customer information can subject Birch to legal penalties that may include substantial monetary fines. Employees involved in misuse or inappropriate disclosure of customer information are subject to employee disciplinary action, including possible termination from employment.

Supervisors or employees aware of misuse or inappropriate disclosure of customer information must report that knowledge to a member of the Birch Legal and Regulatory Department when such misuse or inappropriate disclosure is discovered.