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

Annual 64.2009(e) CPNI Certification for 2016 covering the prior calendar year 2015

1. Date filed: February 24, 2016
2. Name of company covered by this certification: Lycom Communications, Inc.
3. Form 499 Filer ID: 828608
4. Name of signatory: Steven Lycans
5. Title of signatory: Secretary and General Manager
6. Certification:

I, Steven Lycans, certify that I am an officer of Lycom Communications, Inc. ("Lycom"), and, acting as an agent of Lycom, that I have personal knowledge that Lycom has established operating procedures, as summarized in the attached statement, that are adequate to ensure compliance with the customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq*.

Attached to this certification is an accompanying statement explaining how Lycom's procedures ensure that the it 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.

Lycom has not received any customer complaints in the past calendar year concerning unauthorized release of CPNI. Lycom does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Lycom has therefore not taken any actions in the past year against data brokers, including proceedings instituted or petitions filed by the company at either state commissions, the court system or at the Commission.

I hereby represent and warrant that the above certification is consistent with Section 1.17 of the Commission's rules, 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject Lycom to enforcement actions.

Steven Lycans
General Manager
Lycom Communications, Inc.
Executed February 23, 2016

CPNI Compliance Policies of Lycom Communications, Inc.

The following summary describes the policies of Lycom Communications, Inc. ("Lycom") that are designed to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq*. CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

This disclosure does not apply to Lycom's practices with respect to CPNI associated with its broadband Internet access services, which became subject to the requirements of Section 222 of the Communications Act effective June 12, 2015, but which are not subject to the FCC's CPNI rules. Lycom is committed to engaging in reasonable, good-faith steps to protect broadband CPNI from unauthorized use or disclosure.

These policies are managed by Lycom's CPNI Compliance Manager, Steven Lycans, General Manager.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Lycom will use, disclose, or permit access to individually identifiable CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of Lycom, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide inside wiring installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Lycom does not use CPNI to market service offerings among the different categories of service, or even within the same category of service, that it provides to subscribers. Although Lycom's current policy is not to use CPNI for marketing, in the event that any employee or agent wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use is subject to a supervisory review process that shall involve the CPNI Compliance Manager. If such use is approved, Lycom shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

Lycom does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

When Lycom receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, Lycom will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Lycom's existing policies that would strengthen protection of CPNI, they should report such information immediately to the CPNI Compliance Manager so that Lycom may evaluate whether existing policies should be supplemented or changed.

A. Online Accounts

When a customer submits a request for new telephone service, they must provide an email address that will serve as an address of record for their telephone account. An email is sent to the new customer's email address of record that includes a unique secure link that can be used to access on-line account through which the customer may obtain or update certain account information.

The customer is initially authenticated through the use of this link. Upon initial entry into the on-line portal through this link, the customer is required to choose a password and a CPNI Authentication Passcode. After the user chooses a password, the authentication link sent to the customer expires and no longer provides entry into the account, which thereafter can only be accessed by correctly providing the login ID and password. The site instructs the user to select a password and Passcode that do not consist of any significant portion of the customer's name, family names, account number, telephone number, street address, zip code, social security number, date of birth, other biographical or account information, or easily guessed words or strings of digits.

A password and/or the CPNI Authentication Passcode may be changed by the user after logging into the online account with the correct login ID and password.

If a customer forgets their password, they may enter their CPNI Authentication Passcode to have their login credentials sent to their address of record. If they have also do not have their CPNI Authentication Passcode, they may only obtain these credentials by contacting company by phone and asking for these credentials to be provided by a return telephone call to the telephone number of record for the account, or sent to the address of record that has been on file for 30 days, or they may visit a Company office and present photo identification that meets the requirements of Section II.B. herein.

B. Inbound Calls to Lycom Requesting CPNI

CSRs may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated.

More stringent protections apply to Call Detail Information (CDI), which includes 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 any call. Even after a caller has been authenticated under the process above, Lycom does not reveal CDI to an inbound caller. Instead, if an inbound caller requests CDI, the CSR will first encourage them to obtain the information from their online account. If the caller is unable or not interested to obtain the information from their online account, Lycom may offer to provide the requested CDI by sending the information by mail to a mailing address of record for the account, but only if such address has been on file with Lycom for at least 30 days. Alternatively, a customer may obtain CDI at a Lycom office in accordance with Section II.C below.

C. In-Person Disclosure of CPNI at Lycom Offices

Lycom may disclose a customer's CPNI to an authorized person visiting a Lycom office upon verifying that person's identity through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) matching the customer's account information.

D. Notice of Account Changes

Whenever a password or online account is created or changed, Lycom will provide a notice to a customer address of record. Whenever a postal or e-mail address of record is created or changed, Lycom will send a notice to customer's prior address of record notifying them of the change. The foregoing notifications are not required when the customer initiates service, including the selection of an email address or creation of an online account at service initiation.

Each of the notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Lycom if they did not authorize the change.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Lycom employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the CPNI Compliance Manager. Such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Lycom's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Lycom's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If a Lycom employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Lycom's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. The CPNI Compliance Manager will determine whether it is appropriate to update Lycom's CPNI policies or training materials in light of any new information; the FCC's rules require Lycom on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. Lycom's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450) for instructions.

Lycom will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below. (A full business day does not count a business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure.

If Lycom receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Lycom will delay notification to customers or the public upon request of the FBI or USSS. If the CPNI Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Lycom still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

IV. RECORD RETENTION

The CPNI Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must 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.

Lycom maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Lycom later changes its policies to permit the use of CPNI for marketing, it will revise its recordkeeping policies to comply with the Commission's recordkeeping requirements.

Lycom maintains a record of all customer complaints related to their handling of CPNI, and records of Lycom's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that Lycom considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Lycom will have an authorized officer, as an agent of Lycom, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Lycom has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC by the first business day or on after March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Lycom's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must 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. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

All employees with access to CPNI receive a copy of Lycom's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Lycom requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.