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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering prior calendar year 2017

Date filed: February 16, 2018

Name of company(s) covered by this certification: Socket Telecom LLC

Form 499 Filer ID: 824564

Name of signatory: Carson Coffman

Title of signatory: President & COO

I, Carson Coffman, 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 

Attachments: Accompanying Statement explaining CPNI procedures

STATEMENT REGARDING
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI)
OPERATING PROCEDURES

This statement explains the operating procedures Socket Telecom LLC ("Socket") to ensure compliance with the Customer Proprietary Network Information ("CPNI") rules of the Federal Communications Commission ("Commission" or "FCC").

Socket uses, discloses and permits access to CPNI for the purpose of providing a customer with the requested telecommunications service. Socket also uses CPNI for various purposes permitted by law, including; (a) to initiate, render, bill, and collect for its telecommunications services; or (b) to protect the rights or property of the Company, or to protect users of those services and other service providers from fraudulent, abusive, or unlawful use of, or subscription to, such services; (c) for purpose of providing carrier premise equipment and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, protocol conversion; and (d) for the provision of inside wiring, installation, maintenance, repair services.

Business customers have a dedicated account representative as a primary contact. The account representative can be reached directly so that the customer is not required to go through a call center. Business customer contracts address the protection of the customer's CPNI. Therefore, business customers are exempt from the FCC's carrier authentication rules.

Residential customers are required to establish a password in order to access their CPNI. Prior to establishing the password, the customer is authenticated and is then permitted to choose a password. In addition, Socket has established procedures for authenticating the customer in the event of a lost or forgotten password, including calling the customer at the telephone of record or by the customer providing legal photo ID at the retail location.

This password is also required in the event the customer seeks access to call detail information through a customer-initiated telephone contact to Socket's call center. If a customer does not provide a password, Socket will only release call detail information by sending the requested information to an address of record or by calling the customer at the telephone of record.

Socket does permit customers to view CPNI information online. To access CPNI online, the customer must enter a valid USER ID and password.

In addition, all CPNI information stored in Socket's databases is password protected and only employees with a need to access this information are permitted to do so. Passwords are encrypted and stored. They may only be retrieved by an exact match. Socket's system will not permit forgotten passwords to be retrieved. Instead, in the event a customer forgets a password, the customer must be validated using one of the permitted methods and establish a new password.

Within 5 days of an instance where a customer's ability to opt-out does not work properly, Socket will notify the Commission by letter with a description of the mechanisms used, the problem experienced, the remedy proposed, and when the remedy was or will implemented. A copy of the notice to the customer will also be provided, along with a description of whether the relevant state commission has been informed and what action they have taken.

Socket Telecom does not share CPNI information between affiliates, joint-venture partners, or independent contractors.

Socket Telecom maintains records for at least one year of their own sales and marketing campaigns that use their customers' CPNI. Such records include a description of each campaign, the specific CPNI that was used in the campaign and what products and services were offered as a part of the campaign. All marketing campaigns must go through a review process before being approved. The proposals for these campaigns, and information released for approved campaigns are kept in their written or electronic form. Once a marketing campaign or event has been approved, only CPNI information that is permissible to be used in campaign will provided for use in that campaign.

Within 5 days of a reasonable determination of breach *(i.e.,* CPNI disclosed to a third party without customer authorization), Socket will notify the US Secret Service ("USSS") and Federal Bureau of Investigation ("FBI") of the breach via the central reporting facility www.fcc.gov/eb/cpni. After 5 days of USSS and FBI notice, if the Socket has not received written direction from USSS or FBI, Socket will notify the customer of the breach, unless the USSS and FBI have extended the period for such notice. For 2 years following USSS and FBI notice, the Company will maintain a record of (1) discovered breaches; (2) notifications to USSS and FBI; (3) USSS and FBI responses; (4) dates breaches discovered; (5) dates the Company notified USSS and FBI; (6) details of CPNI breached; and (7) circumstances of breaches.

Socket Telecom employees are trained as to the proper protection, uses and treatment of CPNI. Socket employs appropriate remedies against those persons violating the CPNI policies and procedures, including, but not limited to, financial, legal or disciplinary actions including termination and referrals to law enforcement when appropriate.