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

EB Docket 06-36

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

Date filed: February 27, 2018

Name of company(s) covered by this certification: SECOM, Inc.

Form 499 Filer ID: 816616

Name of signatory: Jon Saunders

Title of signatory: Chief Operations Officer

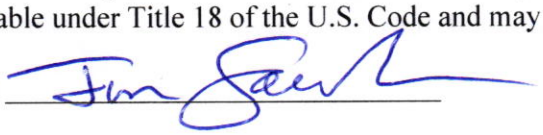
I, Jon Saunders, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et 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 (including those mandating the adoption of CPNI procedures, training, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company *has not* taken actions (*i.e.,* 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.

The company *has not* received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Attachments: Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers (if applicable)
Summary of customer complaints (if applicable)

ACCOMPANYING STATEMENT

This statement explains how SECOM, Inc. (the Company's) procedures ensure compliance with the FCC's rules on CPNI and the safeguarding of such customer information.

The Company's operating procedures ensure that it is in compliance with the FCC's CPNI rules because disclosure of, or permitting access to, our customers' CPNI is not allowed without obtaining the requisite customer approval, except as required by law, or the exceptions set forth in 47 U.S.C. §222, and Subpart U of Title 47 of the Code of Federal Regulations; 47 C.F.R §64.2001 through §64.2011. Appropriate safeguards on the disclosure of CPNI have been implemented in accordance with C.F. R. §64.2010.

The Company has a written CPNI policy that explains what CPNI is, when it may be used without customer approval, and when customer approval is required prior to CPNI being used, disclosed or accessed for marketing purposes.

The Company has assigned a Director for CPNI Compliance to serve as the central point of contact regarding the Company's CPNI responsibilities and questions related to CPNI policy. The Director for CPNI Compliance has responsibilities including, but not limited to, supervising the training of all Company employees with access to CPNI, investigating complaints of unauthorized release of CPNI, and reporting any breaches to the appropriate law enforcement agencies. The Director for CPNI Compliance also maintains records in accordance with FCC CPNI rules, including records of any discovered breaches, notifications of breaches to law enforcement, and law enforcements' responses to the notifications, for a period of at least two years.

The Company has internal procedures in place to educate its employees about CPNI and the disclosure of CPNI. Employees with access to this information are trained on the FCC's rules and are prohibited from disclosing or permitting access to CPNI without the appropriate customer consent. In accordance with Company policy, any employee that uses, discloses, or permits access to CPNI in violation of Federal regulations is subject to disciplinary action, and possible termination. The Company's CPNI policy manual describes the disciplinary process related to noncompliance with CPNI obligations.

The Company requires express opt-in consent from a customer prior to the release of CPNI to a joint venture partner or independent contractor for marketing purposes. However, currently, the Company has not and does not plan to release CPNI to any third parties for marketing purposes.

The Company's policy is to maintain records of customer approval for use of CPNI, as well as customer notification of their right to restrict use of, disclosure of, and access to that customer's CPNI, for a minimum of one year. The Company maintains records of customer approval and disapproval for use of CPNI in a readily available location so the status of a customer's approval can be clearly established prior to use of CPNI.

The Company's policy is to maintain records of its own and its affiliate sales and marketing campaigns that use CPNI. The Company's policy is to maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. These records include a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. The Company maintains these records for a minimum of one year.

The Company has a supervisory review process regarding compliance with the FCC's rules relating to protection of CPNI for outbound marketing situations. The purpose of this supervisory review process is to ensure compliance with all rules prior to using CPNI for a purpose for which customer approval is required. The Company's sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

The Company will provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that customers' inability to opt-out is more than an anomaly. The notice will be in the form and content required by Section 64.2009 (f)(1) of the Commission's rules, and will be submitted even if the Company offers other methods by which customers may opt-out.

Appropriate safeguards on the disclosure of CPNI have been implemented in accordance with C.F.R. §64.2010. Prior to the disclosure of CPNI, customers initiating calls to or visiting the Company's offices are properly authenticated. Passwords and password back-up authentication procedures for lost or forgotten passwords are implemented in accordance with §64.2010(e). To establish a password for an existing customer, the Company must first authenticate the customer without the use of readily available biographical information, or account information, such as calling the customer back at their telephone number of record. For a new customer, the password would be established at the time of service initiation.

Call detail information is only disclosed over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the Company asking for readily available biographical information, or account information. If the customer does not provide a password, call detail information is only provided by sending it to the customer's address of record or by calling the customer at their telephone number of record. 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 is permitted to discuss the call detail information provided by the customer. Prior to the Company disclosing CPNI to a customer visiting any of its retail offices in person, the customer must present a valid photo ID matching the customer's account information.

The Company does not rely on readily available biographical information or account information to authenticate a customer's identity before a customer can access CPNI related to their telecommunications account online. Once authenticated, a customer can only obtain online access to CPNI related to his or her telecommunications account with a password that is not prompted by the Company asking for readily available biographical information, or account information.

The Company has implemented procedures to notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, or address of record is created or changed.

In the event of a CPNI breach, the Company complies with the FCC's rules regarding notice to law enforcement (i.e., United States Secret Service and the Federal Bureau of Investigation) and customers. Records of any CPNI breach and notifications to law enforcement, notifications made to customers, as well as law enforcement's responses are maintained for a period of at least two years.