MINTZ LEVIN

Russell H. Fox | 202 434 7483 | rfox@mintz.com

701 Pennsylvania Avenue, N.W.
Washington, D.C. 20004
202-434-7300
202-434-7400 fax
www.mintz.com

January 26, 2009

BY ELECTRONIC COMMENT FILING SYSTEM

Marlene Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Norcom Communications Annual CPNI Certification 2009

Dear Ms. Dortch:

As required by the rules of the Federal Communications Commission at 47 C.F.R.§ 64.2009(e), attached is the annual Customer Proprietary Network Information (CPNI) Certification from Norcom Communications Corp. Please contact the undersigned with any questions or need for additional information.

Respectfully submitted,

Russell H. Fox

Attachment

NORCOM COMMUNICATIONS CORP.

70-C Corbin Avenue, Bay Shore, New York, 11706 • (631) 595-2555

Annual 17 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed:

Name of company covered by this certification: **Norcom Communications Corp.**

Form 499 Filer ID: **821962**

Name of signatory: **Douglas Nopper**

Title of signatory: **President**

I, Douglas Nopper, 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 _____

Norcom Communications Corp. Explanation of Compliance with FCC CPNI Rules

To ensure compliance with Federal Communications Commission ("FCC" or "Commission") rules and orders governing protection, use, and disclosure of customer proprietary network information ("CPNI"), Norcom Communications Corp. ("Norcom" or the "Company") has adopted the attached CPNI Policy and Employee Guidelines ("CPNI Policy"). An officer of the Company has been assigned responsibility for ensuring that the CPNI Policy is consistently followed, that CPNI complaints and problem reports are appropriately responded to, and that all required reports to law enforcement and the FCC are timely made. All employees that have access to customers or customer data are made aware of the CPNI Policy through review of the policy and its requirements. A copy of the CPNI Policy has been provided to each such employee.

The CPNI policy does not include rules for protection of CPNI in marketing uses because Norcom does not use or allow others to use its customers' CPNI for marketing of any kind. The CPNI Policy does not include provisions for password protection for disclosure of call detail information by telephone because Norcom does not provide any CPNI by telephone. The CPNI Policy does not include provisions for password protection for disclosure of CPNI online because Norcom does not provide access to any CPNI online. The CPNI Policy does not include provisions for regulating customer access to CPNI in person at retail outlets because Norcom does not maintain any retail outlets.

NORCOM COMMUNICATIONS CORP.

70-C Corbin Avenue, Bay Shore, New York, 11706 • (631) 595-2555

Safeguarding Customer Proprietary Network Information:

Policy and Employee Guidelines

***Policy Statement*:** It is the policy of Norcom Communications Corp. ("Norcom" or the "Company") 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 Norcom employees only as permitted by applicable federal regulations and Norcom procedures as described below.

***Types of customer information protected*:** During the course of a customer's relationship with Norcom, 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 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 Norcom without the customer's express permission. Within Norcom, customer information will be used only for the purpose of providing customer service as described below. Norcom does not use, or allow others to use, customer information for the purpose of marketing to its customers.

***Types of customer permission required*:** Upon written request from the customer, the customer's information may be disclosed to any person designated by the customer. Customer information will not be released to a customer over the phone. Customers may, over the phone or in writing, request that Norcom send call detail information to the customer's postal or e-mail address of record, or request that Norcom call the customer's telephone number of record with the requested information.

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

***Exceptions to use and disclosure restrictions*:** Norcom will use or disclose customer information without permission only 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 protect Norcom, its customers, or other parties against fraudulent, abusive or unlawful use of services; or
3. 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 purpose #1, above. Supervisors faced with a situation described in purposes #2 or #3 should consult with the Company's counsel 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 the Company's counsel.

***Employee Training*:** As part of initial orientation and training, all new employees will be informed of Norcom's policies and procedures with regard to protection and appropriate access and use of customer information.

***Required Notifications and Annual Certification*:** To allow a customer to verify that any change of proprietary information was intentional, the Company will notify a customer immediately, through telephone call to the customer's number of record or mail to the customer's address of record,[2/] of any changes to the customer's address of record.

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 the Company's counsel. The Company's counsel will, no later than seven days after determination of the breach, notify law enforcement through an online central reporting facility maintained by the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"). Unless instructed otherwise by law enforcement, Norcom will notify the customer of the breach seven days after reporting it to the USSS and FBI.

The Company will, by March 1st of each year, execute the required certification of Norcom'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.

[2/] A customer's address of record may be any address, either postal or electronic (*i.e.*, e-mail), that has been associated with the customer's account for at least 30 days. The telephone number of record must be the number associated with the underlying service, and not some other number the customer has given as "contact information."

***Penalties for misuse or inappropriate disclosure of customer information; reporting misuse*:** Misuse or inappropriate disclosure of customer information can subject Norcom 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 the president of Norcom when such misuse or inappropriate disclosure is discovered.