CROCKER & CROCKER
ATTORNEYS AT LAW

PATRICK D. CROCKER
patrick@crockerlawfirm.com

February 20, 2014

Ms. Marlene H. Dortch, Commission Secretary
Federal Communications Commission
445 12th Street, SW, Suite TW-A325
Washington, DC 20554

Filed Electronically Via ECFS

RE: American Telecommunications Systems, Inc.
Customer Proprietary Network Information Certification
EB Docket No. 06-36

Dear Ms. Dortch:

American Telecommunications Systems, Inc., by its undersigned attorneys, hereby submits its 2013 CPNI Compliance Certificate and Accompanying Statement certifying compliance with Section 64.2001 *et seq.* of the Commission's rules.

Please contact the undersigned should you have any questions or concerns at (269) 381-8893 extension 226 or patrick@crockerlawfirm.com.

Very truly yours,

CROCKER & CROCKER

Patrick D. Crocker

PDC/tld

Enclosures

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2014 covering the prior calendar year 2013

Date filed: February 18, 2014

Name of Company Covered by this Certification: American Telecommunications Systems, Inc.

Form 499 Filer ID: 818356

Name of Signatory: Bill Stathakaros

Title of Signatory: President

I, Bill Stathakaros, 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, 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.

This Certification is dated this 18th day of February, 2014.

Bill Stathakaros
President
American Telecommunications Systems, Inc.

ACCOMPANYING STATEMENT

American Telecommunications Systems, Inc.'s ("ATS") operating procedures ensure that ATS is in compliance with the requirements set forth in the Commission's CPNI rules as set forth in 47 C.F.R. Part 64, Subpart U (the "**CPNI Rules**") as follows:

- ATS's operating procedures prohibit the use, disclosure or release of CPNI, except as permitted or required under 47 U.S.C. § 222(d) and Rule 64.2005. ATS does not use disclose or permit access to CPNI for any purpose (including marketing communications-related services) and does not disclose or grant access to CPNI to any party (including to agents or affiliates that provide communications-related services), except as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.

- ATS's operating procedures prohibit the use of CPNI in sales or marketing campaigns. ATS does not use, disclose or grant access to CPNI for any purpose, to any party or in any manner that would require a customer's "opt in" or "opt out" approval under the Commission's CPNI Rules. ATS does not currently solicit "opt in" or "opt out" customer approval for the use or disclosure of CPNI.

- ATS takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. ATS's operating procedures include safeguards designed to identify and protect against unauthorized use, disclosure or access to CPNI. ATS authenticates a customer prior to disclosing CPNI based on customer-initiated telephone contact or an in-store visit.

- ATS maintains a record of all instances where CPNI was disclosed or provided to third parties and where third parties were permitted access to CPNI. Records of all instances where CPNI was disclosed or provided to third parties, or where third parties were permitted access to CPNI, are maintained for a minimum of one year.

- ATS does not release call detail CPNI over the telephone, based on customer-initiated telephone contact, unless the customer first provides a password that is not prompted by ATS asking for readily available biographical information or account information or unless the customer is able to provide the relevant call detail information without ATS assistance. If a customer does not provide a password and is not able to provide the relevant call detail information without ATS assistance, ATS only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

- ATS provides customers with access to CPNI at ATS's retail locations only if the customer presents a valid photo ID and the valid photo ID matches an authorized name on the customer account. If a customer is not able to provide a valid photo ID, he or she may instead provide the account password in the same manner required for customer-initiated telephone contact. If a customer is not able to provide a valid photo ID or account password in connection with an in person inquiry, ATS only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

- ATS has established a system of passwords and password protection. For a new customer establishing service, ATS requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, ATS must first authenticate the customer without the use of readily available biographical information or account information, for example by calling the customer at the telephone Number of record or by using a personal identification number (PIN) or similar method to authenticate a customer.

- If a customer password is forgotten or lost, ATS uses a backup customer authentication method that is not based on readily available biographical information or account information.

- If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based on a customer-initiated telephone call by asking ATS to send the call detail information to an address of record or by ATS calling the customer at the telephone number of record. If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based on personal inquiry at a retail location by providing a valid photo ID that matches an authorized name on the customer account or by asking ATS to send the call detail information to an address of record or by ATS calling the customer at the telephone number of record.

- ATS has procedures and policies in place to notify a customer immediately when a password, customer response to a back-up means of authentication, address of record or other critical account information is created or changed.

- ATS does not currently provide online account access to customers.

- All ATS employees with access to or a need to use CPNI have been trained regarding ATS's operating procedures and as to when they are and are not authorized to use, disclose or permit access to CPNI. ATS's employees have been trained regarding the types of information that constitute CPNI and ATS's safeguards (such as employee restrictions, password protection, supervisory review, etc.) applicable to ATS's handling of CPNI. ATS's employee manual includes a disciplinary policy requiring compliance with ATS's operating procedures and sets forth penalties for noncompliance, up to and including termination of employment.

- ATS has appointed a compliance officer and established a supervisory review process regarding ATS's compliance with the Commission's CPNI Rules. ATS's operating policies require that employees confer with the compliance officer if they are unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI. ATS's operating policies require that the compliance officer confer with ATS's legal counsel if he or she is unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI.

- ATS's compliance officer has personal knowledge of ATS's operating procedures and is authorized, as an agent of ATS, to sign and file an annual CPNI compliance certification with the Commission.

- All ATS employees and the compliance officer are trained to identify and protect against activity that is indicative of pretexting. All ATS employees and the compliance officer are required to report any breach or potential breach of CPNI safeguards and/or any customer complaints regarding CPNI. In the event of a CPNI breach, ATS's operating procedures require compliance with the Commission's CPNI Rules regarding notice to law enforcement and customers. ATS must maintain records of any discovered breaches and notifications to the Secret Service and the FBI regarding those breaches, as well as the Secret Service and the FBI responses to such notifications, for a period of at least two years.