



February 10, 2010
VIA ECFS

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

RE: EB Docket No. 06-36
2009 CPNI Certification Filing for STS Telecom, LLC

Dear Ms. Dortch:

In accordance with Federal Communications Commission's Enforcement Advisory No. 2010-01, DA 10-91, EB Docket No. 06-36, released January 15, 2010 and pursuant to 47 C.F.R. § 64.2009(e), **STS Telecom, LLC** files its Certification and supporting Statement of Customer Proprietary Network information (CPNI) for the year 2009. Please include this Certification in EB Docket No. 06-36.

Please contact me at 407-740-3031 or stthomas@tminc.com if you have any questions about this filing.

Sincerely,

/s/Sharon Thomas
Sharon Thomas
Consultant to STS Telecom, LLC

ST/im.

Enclosure

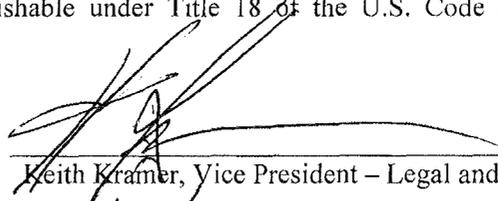
cc: Best Copy and Printing FCC@BCPIWEB.COM
Keith Kramer, STS Telecom
File: STS Telecom - FCC CPNI
TMS: FCC1001

**ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE**

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2010:	Covering calendar year 2009
Name of company(s) covered by this certification:	STS Telecom, LLC
Form 499 Filer ID:	825590
Name of signatory:	Keith Kramer
Title of signatory:	Vice President – Legal and Regulatory

1. I, Keith Kramer, 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.*
2. 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 §64.2001 *et seq.* of the Commission's rules.
3. 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.
4. The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.
5. 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.



Keith Kramer, Vice President – Legal and Regulatory

2/9/2010

Date

Attachments: Accompanying Statement explaining CPNI procedures

Attachment A
Statement of CPNI Procedures and Compliance

STS Telecom, LLC

Statement of CPNI Procedures and Compliance

STS Telecom, LLC (“STS” or “the Company”) does not use or permit access to CPNI to market any services outside of the total service approach as specified in 47 CFR §64.2005. If STS elects to use CPNI in a manner that does require customer approval, it will follow the applicable rules set forth in 47 CFR Subpart U, including the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

The Company trains its employees as to when they are and are not authorized to use CPNI. Employees receive this training during their new employee initiation and in annual refresher training. STS has a strict disciplinary process in place for the unauthorized use or improper disclosure of CPNI, which includes suspension or immediate dismissal of employees who violate the Company policy.

STS maintains a record of all sales and marketing campaigns that use CPNI. All outgoing marketing campaigns are reviewed and must be approved by the Company’s internal Regulatory Affairs Executive who is knowledgeable regarding CPNI requirements, prior to initiation of the campaign.

STS does not disclose CPNI to any agents, affiliates, joint venture partners or independent contractors, nor does it use CPNI to identify or track customers who call competing providers. The Company has a strict policy prohibiting the disclosure of CPNI to any third parties, unless required to do so by law (e.g., in response to a subpoena). The Company maintains a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI pursuant to legally authorized requests.

The Company has instituted authentication procedures to safeguard the disclosure of call detail over the telephone. Customers are authenticated by the Company’s account manager or agent at the time of service initiation, when the customer’s identify is readily authenticated. At that time, at the customer’s request, a password is issued, which does not rely upon readily available biographical information or account information. STS has also established back-up authentication procedures for lost or forgotten passwords that utilize pass code questions that do not rely upon readily available biographical information or account information.

If the appropriate password is not provided, STS does not disclose call detail over the telephone in response to a customer-initiated inquiry, unless the customer can provide the call detail information that is the subject of the inquiry without the assistance of a customer service representative.

STS has instituted authentication procedures to safeguard the disclosure of CPNI on-line. These procedures do not require the use of readily available biographical information or account information as defined by the FCC. The company authenticates customers at the time of service initiation when the customer establishes a password for online access. Passwords do not rely on readily available biographical information or account information. Unless the appropriate password is provided, STS does not allow on-line access to CPNI. If a customer loses or forgets their password, the customer's identify is re-authenticated without the use of readily available biographical information or account information.

STS immediately notifies customers whenever a password, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information.

STS does not have any retail locations and therefore does not disclose CPNI in-store.

The Company has procedures in place to notify law enforcement in the event of a breach of customers' CPNI and to ensure that the affected customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. Specifically, as soon as practicable, and in no case later than seven business days upon learning of a breach, the company will notify the U.S. Secret Service and the FBI by electronic means, as required by FCC regulations. The company will not notify customers or disclose a breach to the public until seven full business days have passed after notification to the U.S. Secret Service and the FBI, unless it believes there is an extraordinarily urgent need to notify customers before seven days in order to avoid immediate and irreparable harm. In that instance, it will only notify such customers *after* consultation with the relevant investigating agency and will cooperate with the agency's request to minimize any adverse effects of the customer notification. If the Company receives no response from law enforcement after the seventh full business day, it will promptly proceed to inform the customers whose CPNI was disclosed of the breach. The company will delay notification to customers or the public if requested to do so by the U.S. Secret Service or FBI. Notifications to law enforcement and customers are handled by a designated supervisor level employee responsible for managing the company's CPNI compliance.

The Company has not had any breaches of its customers' CPNI during the past year, but does have processes in place to ensure that it maintains electronic records of any breaches that are discovered and of notifications made to the USSS and the FBI, as well as to customers, for a period of at least two years. Information regarding any breaches and notifications will be maintained by a designated supervisor level employee responsible for managing the company's CPNI compliance.

The Company has not taken any actions against data brokers in the last year.

STS did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2009.

To date, the Company has not developed any information with respect to the processes pretexters are using to attempt to access CPNI. However, all employees undergo training to recognize pretexters' methods, as outlined by the FCC. The company utilizes its quality assurance call monitoring as one method of detecting potential pretexting.