CROCKER & CROCKER, P.C.
ATTORNEYS AT LAW

**PATRICK D. CROCKER**
patrick@crockerlawfirm.com

February 22, 2011

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

*Filed Electronically Via ECFS*

RE: T3 Communications, Inc.
Customer Proprietary Network Information Certification
EB Docket No. 06-36

Dear Ms. Dortch:

T3 Communications, Inc., by its undersigned attorneys, hereby submits its 2010 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, P.C.

Patrick D. Crocker

PDC/tld

Enclosures

cc: Best Copy and Print, Inc. (via e-mail FCC@BCPIWEB.COM)

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

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2010

Date filed: February 22, 2011

Name of Company Covered by this Certification: T3 Communications, Inc.

Form 499 Filer ID: 823658

Name of Signatory: Josh Reel

Title of Signatory: CEO

I am the CEO of T3 Communications, Inc. and as such do hereby certify, affirm, depose, and say that I have authority to make this Customer Proprietary Network Information ("CPNI") Annual Certification of Compliance on behalf of T3 Communications, Inc. I have personal knowledge that T3 Communications, Inc. has established adequate operating procedures to ensure compliance with the Commission's CPNI rules as set forth in 47 C.F.R. § 64.2001 et. seq.

Attached to this Certification is an Accompanying Statement explaining how the company's procedures ensure compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

T3 Communications, Inc. received no customer complaints in the past year concerning the unauthorized release of CPNI. Further, T3 Communications, Inc. has taken no action against data brokers for the unauthorized release of CPNI during calendar year 2010. T3 Communications, Inc. will report any information it may obtain with respect to the processes pretexters are using to attempt to access CPNI and what steps T3 Communications, Inc. is taking to protect CPNI.

This Certification is dated this 22 day of February, 2011.

Josh Reel
CEO
T3 Communications, Inc.

T3 Communications, Inc. – FCC 499 Filer ID: 823658

2401 First Street
Ft. Myers, FL 33901

**STATEMENT OF FCC CPNI RULE COMPLIANCE**

This statement serves to explain how T3 Communications, Inc., (the "Company") is complying with Federal Communications Commission ("FCC") rules related to the privacy of customer information. The type of information for which customer privacy is protected by the FCC's rules is called "customer proprietary network information" ("CPNI"). The FCC's rules restricting telecommunications company use of CPNI are contained at Part 64, Subpart U of the FCC's rules (47 C.F.R. §64.2000-2011).

## 1. Duty to Protect CPNI

We recognize our duty to protect customer CPNI. We may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

i. Administrative use: We may use CPNI to initiate, render, bill and collect for communications services.
ii. Protection of carrier and third parties: We may use CPNI to protect the interests of our company, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.
iii. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

## 2. Our Use of CPNI in Marketing

The Company does not use CPNI for marketing purposes except in the following circumstances:

i. to market services to our existing customers within the categories of service to which the customer already subscribes;
ii. to market "adjunct-to-basic" services; and
iii. to provide CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

For marketing purposes for which use of CPNI would otherwise require permission from the customers, the Company uses only Customer billing name and address and/or telephone number without any segregation or refinement based on CPNI.

On inbound and administrative call, however, the Company may utilize CPNI in its sales and marketing efforts by first requesting permission to do so pursuant to §64.2008(f). In those cases, the Company recognizes that permission to use CPNI ends when the call terminates and the Customer is fully informed that he may refuse the permission.

We regularly review our marketing practices to determine when, how and if CPNI is used within the Company to insure that we remain in compliance with the FCC's CPNI regulations and with our policy as described here in. In the unlikely event that Company decides to modify its policies for use of CPNI, it will insure that its new policy fully complies with FCC CPNI rules including, but not limited to, tracking and Customer notice provisions contained in §64.2008-2009.

## 3. Authentication Prior to Disclosure of CPNI

We understand that we are required to determine that any request for CPNI will not be released without authenticating the authority of the requestor to receive such information.

We understand that when a customer calls, we may not release CPNI until we have authenticated the release of the information to the requestor in one of the following ways:

i. By calling the customer back at the telephone number associated with the communications service;
ii. By mailing the information to the address of record;
iii. By releasing it in person following authentication via a valid government-issued photo identification at our office;
iv. For those customers who have chosen to do so, over the phone following the disclosure of a password.

## 4. Employee Issues

All of our employees were trained regarding the company's CPNI policies prior to the effective date of the most recent CPNI regulations, December 8, 2007. To maintain compliance with FCC rules after December 8, 2007, the Company developed a manual and identified a compliance officer to address any CPNI-related issues that may arise. The Company has established procedures and trained employees having access to, or occasion to use customer data, to identify what customer information is CPNI consistent with the definition of CPNI under the FCC's revised CPNI rules.

The Company has implemented a training procedure for all new hires and contractors regarding the Company's practices regarding CPNI.

The Company has implemented a training procedure for all new hires and contractors regarding the Company's practices regarding CPNI.

In addition, the Company has in place an express disciplinary process to address any unauthorized use of CPNI where the circumstances indicate the authorization is required under the FCC's CPNI rules.

## 5. Notifications to Customers

We provide a CPNI privacy policy to all customers annually. This policy includes our duty to protect their CPNI and a statement that we do not disclose CPNI to any third parties or use CPNI without their express permission to do so. We also inform them of our requirements for authenticating them prior to disclosing CPNI to them in any way.

We notify customers when changes have been made to passwords, customer responses to back-up means of authentication (if implemented), addresses of record and authorized users by mailing a notification to the account address of record. The notice does not contain information regarding the changes.

## 6. Record-Keeping

We maintain the following records in our files for at least two years:

i. Records relating to the annual mailing of the customer CPNI privacy policy;
ii. Employee disciplinary records, if applicable; and
iii. If applicable: 1) records of discovered CPNI breaches 2) notifications to law enforcement regarding breaches, and 3) any responses from law enforcement regarding those breaches.

## 7. Unauthorized Disclosure of CPNI

We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at http://www.fcc.gov/eb/CPNI/ to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

During the course of the year, we compile information regarding pretexter attempts to gain improper use of CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

Signed:

Josh Reel, CEO

## STATEMENT OF ACTIONS TAKEN AGAINST DATA BROKERS

A. During Calendar Year 2010, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the Federal Communications Commission:

NONE

B. During Calendar Year 2010, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the various Public Utilities Commissions:

NONE

C. During Calendar Year 2010, the Company has instituted the following proceeding, or filed the following petitions, against data brokers before the following federal or state courts:

NONE

## SUMMARY OF CUSTOMER COMPLAINTS REGARDING UNAUTHORIZED RELEASE OF CPNI

A. During Calendar Year 2010, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access by Company employees:

NONE

B. During Calendar Year 2010, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper disclosure to individuals not authorized to receive the information:

NONE

C. During Calendar Year 2010, the Company has received the following number of customer complaints related to unauthorized access to, or disclosure of, CPNI due to improper access to online information by individuals not authorized to view the information:

NONE

D. During Calendar Year 2010, the Company has become aware of the following processes that pretexters are using to attempt to access its CPNI:

NONE