LAW OFFICES OF THOMAS K. CROWE, P.C.
1250 24th STREET, N.W.
SUITE 300
WASHINGTON, D.C. 20037

TELEPHONE (202) 263-3640
FAX (202) 263-3641
E-MAIL firm@tkcrowe.com

February 23, 2012

BY ELECTRONIC SUBMISSION

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

Re: CPNI Certification due March 1, 2012; EB Docket No. 06-36

Dear Ms. Dortch:

STANACARD, LLC, by its undersigned attorney, hereby submits its CPNI compliance certification and accompanying statement, certifying compliance with Section 64.2001 *et seq*. of the Commission's rules.

Should you require further information, please contact the undersigned.

Respectfully submitted,

/s/ Cheng-yi Liu,
Counsel for STANACARD, LLC

Enclosures

cc: Best Copy and Printing, Inc. (fcc@bcpiweb.com)

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2012 covering the prior calendar year 2011

1. Date filed: February 23, 2012
2. Name of company covered by this certification: STANACARD, LLC
3. Form 499 Filer ID: 827594
4. Name of signatory: Manlio Carrelli
5. Title of signatory: Chief Executive Officer
6. Certification:

I, Manlio Carrelli, 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 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.

The company has not received any 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 _____

Manlio Carrelli
Chief Executive Officer

CPNI Compliance Statement

STANACARD, LLC, ("Company") does not use, disclose or permit access to, Customer Proprietary Network Information ("CPNI") except as permitted under 47 U.S.C. § 222(d), except as otherwise required by law pursuant to 47 U.S.C. § 222(c)(1) or except as permitted under 47 U.S.C. §§ 222(c)(1)(A) and 222(c)(1)(B).

A. Definitions

The terms used in this Statement have the same meaning as set forth in 47 C.F.R. § 64.2003.

B. Use of CPNI

(1) The Company does not use, disclose, or permit access to CPNI to market service offerings to a customer that require opt-in or opt-out consent of a customer under 47 C.F.R. § 64.2001 *et seq*.

(2) The Company does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

(3) Notwithstanding the forgoing: It is the Company's policy that the Company may use, disclose, or permit access to CPNI to, among other things, protect the rights or property of the Company, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

C. Safeguards Required for the Use of CPNI

(1) It is the policy of the Company to train its personnel as to the circumstances under which CPNI may, and may not, be used or disclosed. In addition, the Company has established a written disciplinary process in instances where its personnel do not comply with established policies.

(2) In compliance with Section 64.2009(e), the Company will prepare a "compliance certificate" signed by an officer on an annual basis stating that the officer has personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with 47 C.F.R. § 64.2001 *et seq*. The certificate is to be accompanied by this statement and will be filed in EB Docket No. 06-36 annually on March 1, for data pertaining to the previous calendar year. This filing will include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI.

D. Safeguards on the Disclosure of CPNI

It is the Company's policy to take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The Company will properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online access, or in-store visit, if applicable, as described herein.

(1) *Methods of Accessing CPNI.*

(a) *Telephone Access to CPNI.* It is the Company's policy to only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the Company with a password, as described in Section (2), that is not prompted by the carrier asking for readily available biographical information, or account information. 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 may discuss the call detail information provided by the customer.

(b) *Online Access to CPNI.* It is the Company's policy to authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in Section (2), that is not prompted by the Company asking for readily available biographical information, or account information.

(2) *Password Procedures.*

To establish a password, the Company will authenticate the customer without the use of readily available biographical information, or account information. The Company may create a back-up customer authentication method in the event of lost or forgotten passwords, but such back-up customer authentication method will not prompt the customer for readily available biographical information or account information. If the customer cannot provide the correct password or correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

E. Notification of CPNI Security Breaches

(1) It is the Company's policy to notify law enforcement of a breach in its customers' CPNI as provided in this section. The Company will not notify its customers or disclose the breach publicly until it has completed the process of notifying law enforcement pursuant to paragraph (2).

(2) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the Company will electronically notify the United States

Secret Services (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility.

(3) *Recordkeeping*. The Company will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (2), and notifications made to customers. The record will include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. The Company will maintain the record for a minimum of 2 years.