



March 1, 2011  
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  
2010 CPNI Certification Filing for Castle Wire, Inc. f/k/a Business Communication  
Analysts, Inc.**

Dear Ms. Dortch:

In accordance with Federal Communications Commission's Enforcement Advisory No. 2011-02, DA 11-159, EB Docket No. 06-36, released January 28, 2011 and pursuant to 47 C.F.R. § 64.2009(e), Castle Wire, Inc. files its Certification and supporting Statement of CPNI Procedures and Compliance for the year 2010. Please include this Certification in EB Docket No. 06-36.

Please contact me at 407-740-3031 or [sthas@tminc.com](mailto:sthas@tminc.com) if you have any questions about this filing.

Sincerely,

/s/Sharon Thomas  
Sharon Thomas  
Consultant to Castle Wire, Inc.

*ST/im.*

*Enclosure*

cc: Best Copy and Printing [FCC@BCPIWEB.COM](mailto:FCC@BCPIWEB.COM)  
C. Porter, Castle Wire, Inc.  
File: Castle Wire, Inc. - FCC CPNI  
TMS: FCC1101

**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:	Covering calendar year 2010
Name of company(s) covered by this certification:	Castle Wire Inc. f/k/a Business Communication Analysts, Inc.
Form 499 Filer ID:	826466
Name of signatory:	Christopher A. Porter
Title of signatory:	President

1. I, Christopher A. Porter, 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.

  
\_\_\_\_\_  
Christopher A. Porter, President

3/1/11  
\_\_\_\_\_  
Date

**Attachments:** Accompanying Statement explaining CPNI procedures

**Attachment A**  
**Statement of CPNI Procedures and Compliance**

**Castle Wire Inc.**  
**Statement of CPNI Procedures and Compliance**

Castle Wire Inc. (“Castle Wire” or “the Company”) does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. Should Castle Wire elect to use CPNI in future marketing efforts, it will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

Castle Wire 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. Castle Wire does not provide CPNI to third parties, unless the request is made pursuant to a valid subpoena, court order, or other legally authorized request.

Castle Wire has procedures in place to safeguard its customers’ CPNI, including call detail information, from improper use or disclosure; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI. All customer records are maintained on a secure server that is password protected and can only be accessed by a handful of key employees who are aware of the federal requirements to protect this information from unauthorized use or disclosure.

The Company does not disclose CPNI over the telephone in response to a customer-initiated telephone inquiry, unless the customer can provide the pertinent call detail information without the assistance of a customer service representative. If Castle Wire elects in the future to provide telephone access to CPNI in response to a customer-initiated inquiry under any other circumstance, it will establish authentication and password procedures that comply with the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information.

The Company does not disclose CPNI online. If it elects to do so in the future, it will establish authentication and password procedures that are in compliance with the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information.

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

The Company notifies customers whenever an address of record is changed by sending notification of the address change to the old address of record. If the Company in the future provides password-protected access to account information via telephone or online, it will also notify customers immediately via mail or email to the current (not new) address or email address of record whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, or online account is created or changed without revealing the changed information.

The Company did not have any breaches of its customers’ CPNI during 2010, but understands its obligations to notify law enforcement in the event of a breach of customers’ CPNI and to ensure that 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, the Company will notify the U.S. Secret Service and the FBI by electronic means, as required by FCC regulations, as soon as practical and no later than seven business days upon learning of a breach. The Company will not notify customers or disclose a breach to the public until seven full business days have passed after notification to the Secret Service and FBI, unless there is an urgent need for customer notification before that period has elapsed 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 early notification. 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 did not have any breaches of its customers' CPNI during the past year, but will 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.

Castle Wire did not take any actions against data brokers and did not receive any customer complaints about the unauthorized release or disclosure of CPNI in calendar year 2010.

Castle Wire has not developed any information with respect to the processes pretexters are using to attempt to access CPNI.