

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification

Date: February 28, 2013

Name of companies covered by this Certification:

Hughes Telematics, Inc.

Name of signatory: Craig Kaufmann

Title of signatory: Senior Vice President Finance and Treasurer

I, Craig Kaufman, certify that I am an officer of Hughes Telematics, Inc. and acting as an agent of this company, I have personal knowledge that it has established operating procedures, as described in the attached statement, that, to the best of my knowledge, information and belief, and except as noted in the attached statement, 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 this company's current operating procedures are designed to ensure that it is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

Also attached are an explanation of actions, if any, taken against data brokers and a summary of customer complaints received in 2012 concerning the unauthorized release of CPNI.

Signed: _____



Hughes Telematics, Inc.
CPNI Statement of Compliance

Section 64.2005 Use of Customer Proprietary Network Information Without Customer Approval

Hughes Telematics, Inc. (“Hughes”) provides telecommunications services to one customer. Hughes has not used and does not plan to use CPNI for marketing that requires consent.

Sections 64.2007-8 Approval Required for Use of Customer Proprietary Network Information; Notice Required for Use of Customer Proprietary Network Information

Hughes does not use, disclose, or permit access to CPNI to market services that are not within a category of services to which the customer already subscribes. Thus, Hughes does not send notification or request corresponding approval from its customer. Hughes does not use joint venture partners or independent contractors to market to its customer.

Section 64.2009 Safeguards Required for Use of Customer Proprietary Network Information

Hughes trains appropriate personnel about the CPNI rules and advises that the failure to follow them can be grounds for disciplinary action, up to and including dismissal. [Note: All Hughes employees took Code training, which includes CPNI, as of Jan 2013.]

This statement of compliance is preceded by a certificate signed by an officer of Hughes, pursuant to section 64.2009(e). An explanation of actions taken against data brokers and a summary of customer complaints involving instances of the unauthorized release of CPNI is attached below.

Although Hughes currently does not use, disclose, or permit access to CPNI to market services, if it chooses to change this policy and use CPNI for marketing, it will (1) implement a system by which the status of a customer’s CPNI approval can be clearly established, (2) maintain a record of its and its affiliates’ sales and marketing campaigns that use its customers’ CPNI for at least one year, (3) maintain a record of all instances where CPNI was disclosed or provided to third parties for at least one year, (4) require sales personnel to obtain supervisory approval of any proposed outbound marketing request for customer approval, and (5) provide written notice to the FCC within five business days of any instance where its opt-out mechanism did not work properly.

Section 64.2010 Safeguards on the disclosure of customer proprietary network information

Hughes has an assigned representative to work with the single customer receiving telecommunications service. The dedicated Hughes representative discloses CPNI to the customer through a representative authorized by the customer contractually. Hughes does not

provide in-store access or online access to CPNI. Whenever a significant account change occurs, Hughes immediately notifies the customer of the change at an address of record.

Section 64.2011 Notification of customer proprietary network information security breaches

Hughes has implemented procedures to notify law enforcement, and subsequently customers, of CPNI breaches (defined in subsection 64.2011(e)). Internal procedures direct employees to notify the legal department of any potential CPNI breach. When a breach is confirmed, the appropriate personnel are prepared to make the required notifications to the United States Secret Service, the Federal Bureau of Investigation, and the customer. Records of such breaches and the corresponding notifications are maintained for at least two years.

Information Concerning Data Brokers and Complaints of Unauthorized Disclosure

Explanation of Actions Against Data Brokers:¹

Hughes did not take any actions against data brokers in 2012.

Information of Verizon about Processes Used by Pretexters to Access CPNI and Hughes Actions in Response to Protect CPNI:²

Hughes is not aware of any processes used by pretexters not already in the record of the Federal Communications Commission's CPNI docket.

Summary of the Number of Customer Complaints in 2012 Concerning Unauthorized Release of CPNI

A review of allegations revealed no substantiated complaints by customers involving unauthorized access to the customer's CPNI, or unauthorized disclosure of the customer's CPNI:

Number of complaints involving improper access by employees: 0

Number of complaints involving improper disclosure to unauthorized individuals: 0

Number of complaints involving improper online access by unauthorized individuals: 0

¹ Under Commission rules, "actions" are proceedings instituted or petitions filed by a carrier at either state commissions, the court system, or at the Commission against data brokers.

² Under Commission rules, carriers must report information that they have with respect to the processes pretexters are using to attempt to access CPNI, and the steps carriers are taking to protect CPNI.