

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

EB Docket 06/36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2018

1. Date Filed: 03/01/19
2. Name: Impulse Telecom, LLC
3. Form 499 filer ID: 828711
4. Name of signatory: Lynda Radke
5. Title of signatory: CFO
6. Certification: see attached

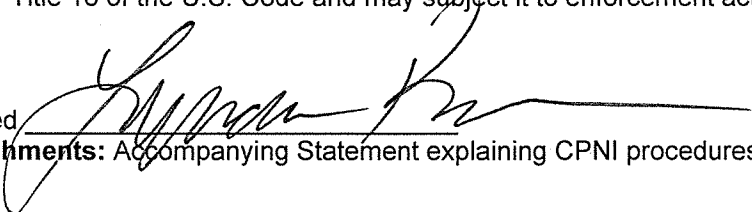
I, Lynda Radke, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

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, safeguards, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules. 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.

The company *has not* received 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

  
**Attachments:** Accompanying Statement explaining CPNI procedures

## **Statement explaining CPNI procedures for Impulse Telecom, LLC**

Impulse Telecom does not make CPNI available to third parties or its affiliates.

**Training** – As part of the new hire process all personnel are put through mandatory training which includes a section that explains the company's CPNI policy. Employees found to have violated the CPNI policy are subject to express disciplinary action up to and including termination of employment.

**Customer Account Protection** – Employees of Impulse Telecom are not allowed to disclose call detail information over the telephone, via email, or by postal mail under any circumstances. Each customer is assigned a dedicated sales account representative. Upon initial account set up, the customer is required to designate an administrative contact and a technical contact for their account, and the technical contact will be provided a unique user name and password that the customer may use to authenticate to an electronic reporting tool to view or download specific call detail records and reports. Inquiries about call detail information from a customer contact other than customer's designated technical contact are then referred to the customer's technical contact. Customers may change their technical contact by contacting an Impulse Telecom billing representative. Any requested changes to a customer's account information including designated contacts, the customer's telephone number or address of record, or the username or password for the electronic reporting tool are verbally confirmed with a telephone call from Impulse Telecom to a listed customer contact at the customer's telephone number of record. This verification does not reveal the changed information.

**CPNI security breaches** – If there is a security breach Impulse Telecom will notify law enforcement and the customers of the details of the breach, in accordance with FCC Rules.

**Recordkeeping** - Impulse Telecom will maintain a record, of any breaches discovered, notifications made to the United States secret Service and the FBI, 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. Impulse Telecom will retain the records for a minimum of 2 years.