



**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 2017

1. Date filed: February 26, 2018
2. Name of company(s) covered by this certification: POPP.com, Inc.
3. Form 499 Filer ID: 802467
4. Name of signatory: Ryan Cummings
5. Title of signatory: VP of Product & Technology
6. Certification:

I, Ryan Cummings, 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 (*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 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 

**Attachments:** Accompanying Statement explaining CPNI procedures



## **STATEMENT OF COMPLIANCE**

The operating procedures of POPP.com, Inc. ensure compliance with the FCC's CPNI Rules. Such procedures are as follows:

### ***Use of CPNI in Marketing***

Our company has implemented a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI. Each customer's record contains a designation identifying whether or not we have obtained, through the processes permitted by the FCC's rules, the customer's approval to use, disclose or permit access to his or her CPNI.

Our company accesses and uses a customer's CPNI to market our own (or our affiliates') communication-related services (outside a customer's current relationship) only after the customer's Opt-Out consent has been obtained in compliance with FCC Rule 64.2008, and which consent has not been revoked by the customer. Every two years our company (a) provides notice of customers' rights to restrict use and disclosure of, and access to, their CPNI, in compliance with FCC Rule 64.2008, and (b) solicits Opt Out consent for the use of the customer CPNI, in compliance with FCC Rule 64.2008, to each customer who has given Opt Out consent.

Our company has a supervisory review process regarding our compliance with the FCC's CPNI rules for any outbound marketing efforts. We require sales personnel to obtain supervisory approval of any proposed outbound marketing request for customer approval.

### ***CPNI Safeguards***

Our company has designated a compliance officer to maintain and secure the company's CPNI records and to supervise training of all company employees.

Our company trains its personnel as to when they are, and are not, authorized to use or disclose CPNI, and we have an express disciplinary process in place if the rules are violated.

Our company authenticates the identity of a customer prior to disclosing CPNI based on a customer-initiated telephone contact, online account access, or in-store visit.

Our company discloses call detail information (CDI) in a customer-initiated call only: after the customer provides a pre-established password; or, at the customer's request, by sending the CDI to the customer's address of record; or by calling back the customer at his or her telephone number of record.

Our company has established password protection for customers' online accounts.

Our company notifies a customer immediately of changes in: a customer's password, a customer's response to back-up means of authentication, online account, or address of record.



### ***CPNI Recordkeeping and Reporting***

Our company is prepared to provide the FCC with written notice, within five business days of any instance where the "opt out" mechanisms do not work properly.

Our company is prepared to notify the U.S. Secret Service and FBI within seven business days after the occurrence of an intentional, unauthorized (or exceeding authorization), access to, use of, or disclosure of CPNI. We may also notify the customer of such breach, after consulting with the investigatory agency(ies), if we believe there is an extraordinarily urgent need to notify a customer (or class of customers) in order to avoid immediate or irreparable harm. We will notify the customer of the breach after 7 business days following notification to the FBI and Secret Service, if such agencies have not requested that we postpone disclosure to the customer.

Our company will maintain records of any discovered breaches, notices to the Secret Service and FBI, and their responses, for at least two years.