

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

Date filed: 02/26/2018

Name of company: Enhanced Communications Network Inc.

Form 499 Filer ID: 821490

Name of signatory: Raymond Chan

Title of signatory: President


I, **Raymond Chan** 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 *ets eq*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules. (**see attached**)

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. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company **has not** received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed x



Raymond Chan
President

Enhanced Communications Network Inc.

Accompanying Statement to Annual CPNI Compliance Certification for
2-26-2018
Enhanced Communications Network Inc

Employee Training and Discipline

- Enhanced Communications Network, Inc. trains and obligates all employees, sales contractors, and sales agents with access to CPNI, to protect the confidentiality of CPNI by requiring compliance with the Enhanced Communications Network, Inc Customer Proprietary Network Information Protection Policy. (the "Policy").
- Enhanced Communications Network, Inc. requires all employees, sales contractors and sales agents with access to CPNI confirm receipt of the Policy, that they have read and understand the Policy. Failure to follow the Policy may result in disciplinary action or termination of the employment.

Sales and Marketing Campaign Approval

- Enhanced Communications Network, Inc. requires management approval for all sales and marketing campaigns.

Record-Keeping Requirements

- Enhanced Communications Network, Inc. implemented a system by which the status of the Customer's CPNI approval can be established prior to the use of CPNI.
- Enhanced Communications Network, Inc. uses the ACT System to maintain a record of all sales and marketing campaigns that use CPNI, including marketing campaigns of affiliates and independent contractors.
- Enhanced Communications Network, Inc. ensured that these records include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign.
- Enhanced Communications Network, Inc. requires that these records are maintained for a minimum of one (1) year.

Establishment of a supervisory Review Process

- Enhanced Communications Network, Inc. established a supervisory review process for all outbound marketing situations.
- Enhanced Communications Network, Inc. certified that under this review process, all sales personnel obtain supervisory approval of any proposed outbound marketing request for the customer approval.

Opt-In

- Enhanced Communications Network, Inc. only discloses CPNI to sales agents, affiliates, joint venture partners, independent contractors, or any other third parties only after receiving "opt-in" approval from the customer.
- Enhanced Communications Network, Inc. enters into confidentiality agreements with joint-venture partners, independent contractors, or any other third party when releasing CPNI. All such confidentiality agreements are reviewed by the director of legal and regulatory affairs.

Opt-Out Mechanism Failure

- Enhanced Communications Network, Inc. established a protocol requiring written notice to the FCC within five (5) business days of any instance where opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.

Compliance Certificates

- Enhanced Communications Network, Inc. executed a statement, signed by an officer, certifying that he has personal knowledge that Enhanced Communications Network, Inc. has established operating procedures that are adequate to ensure compliance with the FCC's CPNI regulations.
- Enhanced Communications Network, Inc. prepared this accompanying Statement detailing how operating procedures ensure compliance with the CPNI regulations.
- Enhanced Communications Network, Inc. provided an explanation of any actions taken against data brokers.
- Enhanced Communications Network, Inc. provided a summary of all customer complaints received in the past year concerning unauthorized release of CPNI.

Customer Authentications Method

- Enhanced Communications Network, Inc. instituted customer authentication methods to ensure adequate protection of CPNI

Customer Notification of CPNI Changes

- Enhanced Communications Network, Inc. established a system under which a customer is notified of any changes to CPNI. The system, at minimum, notifies a customer of CPNI access in the following circumstances:
 - password modification
 - a response to a carrier-designed back-up means of authentication
 - online account changes
 - address of record change or creation

Notification to Law Enforcement and Customers of Unauthorized Access

- Enhanced Communications Network, Inc. established a protocol under which the appropriate law enforcement agency is notified of any unauthorized access to customer's CPNI
- Enhanced Communications Network. ensured that all records of any discovered CPNI breaches are kept for a minimum of two (2) years