



151 Southhall Lane, Ste 450
Maitland, FL 32751
P.O. Drawer 200
Winter Park, FL 32790-0200
www.inteserra.com

March 4, 2019
Via ECFS Filing

Ms. Marlene H. Dortch, FCC Secretary
Federal Communications Commission
9050 Junction Drive
Annapolis Junction, MD 20701

RE: ComStar Technologies, LLC
EB Docket No. 06-36; CPNI Certification for CY 2018

Dear Ms. Dortch:

Attached for filing is the Calendar Year 2018 CPNI Compliance Certification and Statement of CPNI Procedures and Compliance as required by 47 C.F.R. Section 64.2009 (e) submitted on behalf of ComStar Technologies, LLC.

Any questions you may have regarding this filing should be directed to my attention at . Thank you for your assistance in this matter.

Sincerely,

/s/Sharon Thomas

Consultant

tms: FCx1901

Enclosures
im

CPNI Compliance Statement and Operating Procedures of Comstar Technologies, LLC

Pursuant to the requirements contained in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information: IP-Enabled Services*, CC Docket No. 96-115; WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Red 6927 (2007)("EPIC CPNI Order"),¹ I, **Andy Cool, Officer of ComStar Technologies, LLC** makes the following statement:

ComStar Technologies, LLC has established policies and procedures to comply with the Federal Communications Commission's (FCC) rules regarding the use, disclosure, and access to section 64.2001 et seq. of the Commission's rules, 47 C.F.R. §64.2001 et seq. These procedures ensure that Company is compliant with the FCC's customer proprietary network information (CPNI) rules. The purpose of this statement is to summarize our Company's policies and procedures designed to safeguard CPNI.

The Company uses CPNI for the limited purposed of initiating, rendering, billing, and collecting for telecommunications services, and may use CPNI, if necessary, to protect its property rights. Company does not disclose CPNI or permit access to such CPNI to any third parties other than as necessary to provide service.

The 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.

The Company has established procedures to verify an incoming caller's identity. The Company trains its personnel as to when they are and are not authorized to use CPNI, and has an express disciplinary process in place. The Company also limits the number of employees that have access to customer information and call data.

The Company shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must 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.

Carriers shall retain the record for a minimum of one year.

¹ 47 C.F.R. § 64.2009(e) states: "A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certification explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart. In addition, the carrier must include an explanation of any actions taken against data brokers and summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year."

The Company has established a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.

The Company will provide written notice within five (5) business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such A degree that consumers' inability to opt-out is more than an anomaly.

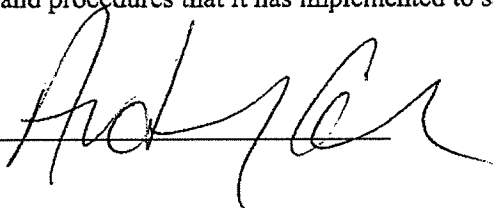
- (1) The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanisms(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.
- (2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

The Company has procedures in place to notify law enforcement in the event of a breach of customers' CPNI and to ensure that the 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, as soon as practicable, and in no case later than seven business days upon learning of a breach, the company will notify the U.S. Secret Service and the FBI by electronic means, as required by FCC regulations. The company will not notify customers or disclose a breach to the public until seven full business days have passed after notification to the U.S. Secret Service and the FBI, unless it believes there is an extraordinarily urgent need to notify customers before seven days in order 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 customer notification. If the Company receives no response from law enforcement after the seventh full business day, it will promptly proceed to inform the customers whose CPNI was disclosed of the breach. 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 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. 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 annually submits a CPNI certification to the FCC from an officer with personal knowledge of the policies and procedures that it has implemented to safeguard CPNI.

/s/ Andy Cool
Andy Cool



Officer
TITLE

DATE

3/4/2019