

Accompanying Statement to Annual 47 C.F.R. § 64.2009(e) CPNI Certification

The Company(s): Virgin Islands Telephone Corporation d/b/a Viya, Vitelcom Cellular, Inc. d/b/a Viya Wireless, and Innovative Long Distance d/b/a Viya Long Distance (“the Company”) adheres to the following guidelines:

General Company Policies

The Company uses, discloses, or permits access to CPNI to protect the rights or property of the Company, or to protect users of services it provides and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

The Company shares CPNI only among the carrier's affiliated entities that provide a service offering to the customer. Except as noted herein, the Company does not share CPNI with its affiliates from which its customer does not take service.

The Company does not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from the Company, unless: (i) the Company has customer approval to do so, or; (ii) such CPNI falls within the exceptions specified in 47 C.F.R. § 64.2005(c), or Section 222(d) of the Communications Act.

Company Policies Regarding the Notice Required for Use of Customer Proprietary Network Information

Prior to any solicitation for customer approval, the Company provides notification to the customer of the customer’s right to restrict use of, disclosure of, and access to that customer’s CPNI.

The Company may seek alternatively either “opt-in” or “opt-out” approval consistent with applicable FCC requirements in order to obtain authorization to use its customer’s individually identifiable CPNI for the purpose of marketing communications-related services to that customer. The Company, subject to opt-out approval or opt-in approval, may disclose its customer’s individually identifiable CPNI, for marketing communications-related services to: that customer; its agents; its affiliates that provide communications-related services; and its joint venture partners and independent contractors. The Company also permits such persons or entities to obtain access to such CPNI for such purposes. Any such disclosure to or access provided to joint venture partners and independent contractors is undertaken in compliance with Joint Venture/Contractor safeguards set forth in Commission rules.

Except for use and disclosure of CPNI that is permitted without customer approval under 47 C.F.R. § 64.2005, or is otherwise permitted under section 222 of the Communications Act of 1934, as amended, the Company uses, discloses, or permits access to its customers’ individually identifiable CPNI subject to opt-out approval in circumstances approved by the FCC.

Company Policies Regarding Safeguards for Use of Customer Proprietary Network Information

Marketing - The Company maintains a record, electronically or in some other manner, of its own and, as may exist, its affiliates' sales and marketing campaigns that use its customers' CPNI. The Company maintains 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 includes 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.

The Company has established a supervisory review process regarding its compliance with applicable FCC rules for outbound marketing situations and maintains records of its compliance with such rules for a minimum period of one year.

Customer Service - The Company has a training program for personnel of when they are and are not authorized to use CPNI. All Company personnel and/or employees are required to follow Company guidelines regarding the confidentiality of CPNI, and the Company will discipline employees for a violation of this policy. The Company also offers a refresher course covering CPNI on an annual basis.

Customer Billing System

CPNI records are maintained in an electronic format in the Customer Billing System with restricted access.

The Company will provide written notice within five business days to the FCC of any instance where the opt-out mechanisms it employs in this process do not work to such a degree that consumers' inability to opt-out is more than an anomaly.

Customer Initiated Telephone Contact

The Company does not release CPNI call detail information (such as the date, the called number, the length of the call etc.) based on a customer-initiated telephone contact unless one of the following criteria apply: (1) the customer provides a pre-established password to the Company customer service representative; the passwords are not publicly available or contain personal history information (such as a social security number or a mother's maiden name) (2) the Company customer service representative calls the customer back at the telephone number of record in order to disclose any requested specific call detail record information; or (3) the Company customer service representative mails the requested call detail information to the customer's address of record.

On-Line Account Access

On-line account access to CPNI call detail records is not available.

Office Location Account Access

Customers requesting CPNI at a location where they walk into a business office must produce a valid photo identification matching the customer of record name on the customer account.

Notice Requirements - Account Changes

The Company has procedures in place to immediately notify a customer of changes to the customer's account, including whenever a password, customer response to a carrier designated back-up means of authentication (*i.e.*, shared secret), online account or address of record is created or changed.

Notice Requirements- Breach of CPNI

If an employee becomes aware of any suspected breach of CPNI protections, he or she is instructed to immediately notify the Compliance Officer for the Company who will then be responsible, in consultation with legal counsel, for determining if we have experienced a breach and then notifying law enforcement which includes the Secret Service and the Federal Bureau of Investigation.

Record of Breaches and Notification

We also keep a record of all discovered breaches and notifications of law enforcement.
We also have procedures in place to notify law enforcement pursuant to FCC rules and procedures.