**Summary of CPNI Compliance and Process Requirements for LPC**

**CPNI Protected Customer Information**

* Numbers called and when (calling records)
* Calling feature utilization

**Approved Circumstances to Use Protected Customer Information**

* When required by law
* When customers provides approval
* As part of providing service (e.g. Caller ID)

**Marketing Restrictions Related to CPNI Rules**

* If and when LPC begins using Customer Information for marketing purposes, we will need to send out an “opt-out” notification to all voice customers.
* At this time, we do not use this information for marketing and I would not expect that we will in the future (e.g. basic customer information such as address, whether the customer subscribes to NextLight voice service or not, etc. is not considered protected information).

**Compliance Reporting Requirements**

* Annually certify to the FCC that the provider is in compliance with CPNI, summarize all complaints from customers regarding unauthorized release of customer information, and any actions taken against data brokers.

**Process Implications**

* Submit annual certification due March 1 of each year
* A password must be established by the customer. Customer information can be discussed only after the password has been provided
* If the password cannot be provided, LPC can mail the information to the address of record, or call back the customer at their phone number of record.
* The customer’s online account, if it includes customer information, must be protected by password access.
* For in person requests for customer information, a valid photo ID must be presented.
* Customer information can be provided to another person if the customer has designated that person, in writing, as being approved by them to receive it.
* The customer must be notified of any password changes and address of record changes.

**Vendor Considerations**

Both GLDS and Alianza systems will separately use their respective CPNI protections.

* We will actively use BroadHub to manage actively all aspects of CPNI regarding customer contact and notifications. The CSRs will not have active involvement with Alianza regarding CPNI aside from fulfilling password reset requests.
* We will passively utilize the CPNI protections embedded in Alianza’s user portal. The site requires the customer to establish an alphanumerical PIN the first time they login. LPC cannot control the PIN or set it to match the BroadHub PIN. If the customer forgets their Alianza PIN, it can be reset by our CSR or TSR. This site allows the phone user to view calling history and manage their calling features/settings. That is protected customer information per the CPNI regs.

Accordingly, for all forms of customer contact (either initiated by LPC or the customer) we will use BroadHub to verify the identity of the information requester.

* Upon writing the initial voice order, the CSR will establish a CPNI PIN or Security Question(s) with the customer and enter it. GLDS accepts either PIN or security question protection as the only forms of “passwords” integrated directly into BroadHub (customer account module).
* For any subsequent contact with the customer that may involve sharing ‘CPNI Protected Customer Information’, the CSR will need to “authenticate” the customer. GLDS supports a number of different approaches to do this, so it is a subjective decision by the system. Authentication is done within the Subscriber Information module of BroadHub.
* GLDS has automated the password change notification requirement via an auto-generated email or letter. These will need to be set up in BroadHub initially, but then will automatically sent the required notifications for CPNI compliance.