

# **POLICY REGARDING CUSTOMER PROPRIETARY NETWORK INFORMATION AND BILLING NAME AND ADDRESS**

## **PURPOSE**

This Policy specifies the circumstances under which the Company, including its affiliates, contractors, and employees, are required to obtain customer approval prior to using, disclosing, or permitting access to customer proprietary network information (“CPNI”) and identifies requirements for obtaining customer approval. This Policy is intended to comply with Section 222 of the Telecommunications Act of 1934, as amended, and with rules of the Federal Communications Commission (“FCC”) governing use and disclosure of CPNI and Billing Name and Address (“BNA”) information.

Both the FCC’s rules and the Telecommunications Act apply to local and to toll services that are provided by a telecommunications carrier or by an affiliate. They also apply to information services that typically are provided by telecommunications carriers, such as Internet access and voice messaging services. Finally, they apply to all providers of interconnected Voice-Over-Internet-Protocol (“VOIP”) service.

## **DEFINITIONS**

Customer means anyone who subscribes to services provided by the Company or who purchases service from the Company.

Customer Proprietary Network Information or CPNI means information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service to which a customer subscribes and that the customer makes available to the Company solely by virtue of the carrier-customer relationship; and information contained in customers’ bills for local or toll service.

Authorized Person means a person who is listed in the account records as a person authorized by the customer to access the customer’s account and to make changes to the customer’s account.

Address On The Account means the address associated with a customer account for at least the prior 30 (thirty) days.

Aggregate Customer Information means collective data that relates to a group of customers or category of service from which individual customer identities and characteristics have been removed. Aggregate customer information is not CPNI.

Billing Name and Address or BNA means the name and address shown on customer bills. BNA is a type of CPNI. It is protected by the CPNI rules and by rules specific to BNA.

Subscriber list information means the information published in the telephone directory, such as telephone number, address, or advertising classification. It is not CPNI.

Interconnected VOIP Service means a service that (1) enables real-time, two-way voice communications, (2) requires a broadband connection from the end user's location, (3) requires Internet Protocol-compatible customer premises equipment, (4) and permits users generally to receive calls that originate on the public switched telephone network and to terminate calls to the public switched telephone network.

Password means a unique series of letters, numerals, or combination of letters and numerals assigned by the Company or selected by the customer to verify his or her identity. Passwords may not contain readily available biographical information about the customer, such as name, address, age, telephone number, maiden name, mother's maiden name, name of a relative, the name of a current pet, school attended, or occupation. Social security numbers cannot be used as passwords.

Pretexting means a person pretending to be a specific customer or authorized person in order to gain access to that customer's CPNI.

Security Breach or Breach means any instance in which a person (including Company personnel), without authorization or exceeding his or her authorization, intentionally gains access to, uses, or discloses CPNI.

Valid, Government-issued Photo Identification means a driver's license, passport, or other document issued by state, federal, or local governments for the purpose of identification and that displays both the name and photograph of the person to be identified. To confirm a person's identity for purposes of this Policy, the name on the identification must match the name of the customer or of an authorized person on the account to be accessed.

The Company means Custer Telephone Cooperative, Inc., its employees, officers, directors, divisions, subsidiaries, and affiliates.

## **CUSTOMERS' CPNI RIGHTS**

Each customer has the legal right to limit, restrict, or prohibit the use of, disclosure of, or access to his or her individual CPNI.

The company has a legal duty to abide by each customer's decision regarding the use, disclosure, or access to his or her CPNI, and to keep records of such decisions.

The company has a legal duty to utilize reasonable measures to protect CPNI from unauthorized access or disclosure, including certain measures that are specifically required by law.

Except as authorized by law and explained below, the Company cannot use, disclose, or permit access to a customer's CPNI without approval from the customer.

## **PROHIBITED USE OF CPNI**

The Company cannot use, disclose, or permit access to customers' CPNI to identify or to track customers who call competing service providers.

## **DISCLOSURE OF CPNI TO CUSTOMERS**

Before a customer's CPNI can be disclosed to a person claiming to be the customer or an authorized person on the account, the identity of the requesting party must be confirmed in a manner authorized under this Policy

### **Special Rule For Customer-Initiated Calls To The Company**

In those instances in which a person who claims to be the customer or an authorized person calls the Company to discuss call detail information contained in a bill or to request CPNI, but cannot confirm his or her identity by one of the approved methods, the Company has three options:

1. mail requested CPNI to the address on the account; or
2. call the served telephone number and orally provide the requested CPNI;
3. discuss with the caller the call detail information provided by the caller, but *only* the information provided by the caller.

Whenever the third option is utilized, Company personnel must not disclose to the caller any additional call detail information or other CPNI, but may perform routine customer care functions related directly to the information provided by the caller.

EXAMPLE 1: A person whose identity cannot be confirmed by an approved method calls the Company to dispute the charge for a toll call. The caller states that a toll call placed to a specific telephone number on September 19<sup>th</sup> at 6:58 P.M. should have been rated at \$0.10 per minute instead of \$0.12 per minute for that portion of the call that occurred after 7:00 P.M. The Company may explain that calls are rated based upon the time they start and that the \$0.10 rate would apply only to calls initiated after 7:00 P.M. The Company also may issue a courtesy credit on the account. But the Company may not do such things as pointing out that a different call on the same bill was rated at \$0.10 because it was initiated at 7:02 P.M., disclosing which calling plan is on the account, and discussing alternative calling plans with the caller.

EXAMPLE 2: A person whose identity cannot be confirmed by an approved method calls the Company to report a service outage at a customer location. The Company may follow routine procedures for handling such reports so long as no CPNI is disclosed about the account. The Company could do such things as confirming whether a service outage has occurred in the area and providing an estimated time when service will be restored, follow routine procedures for determining whether the problem is on the Company side of the demarcation point, and report the problem to repair. The Company cannot do such things as disclose that service has been disconnected for nonpayment.

## **METHODS OF CONFIRMING CUSTOMER IDENTITY**

The identity of a customer or an authorized person can be confirmed only as follows:

### Identity Confirmation at Business Offices or Retail Locations

The identity of a customer or an authorized person can be confirmed for face-to-face interactions by either of the following methods:

- 1) the person presents a valid, government-issued photo identification; or
- 2) the person provides the password for the account.

### Identity Confirmation For Customer-Initiated Telephone Contacts

The identity of a customer or an authorized person can be confirmed during telephone calls placed by the customer or authorized person to the Company only by the caller providing the password or back-up for the account.

### Identity Confirmation For On-Line Account Access

The identity of a customer or an authorized person can be confirmed for purposes of on-line account access only by the person providing the password or back-up for the account.

### Identity Confirmation When Customer Has Forgotten The Password

If a customer or authorized person forgets the password, his or her identity can be confirmed through the use of a back-up method implemented by the Company. If the customer or authorized person also has forgotten the back-up, a new password and back-up must be created using the procedures applicable to an existing customer.

Pending the creation of a new password and backup, the Company may disclose CPNI to a person claiming to be the customer or an authorized person only by:

1. mailing requested CPNI to the address on the account; or
2. calling the served telephone number and orally providing the requested CPNI.

### Identity Confirmation For Business Customers

Business customers generally are subject to the same requirements as residential customers with respect to confirming the identity of the customer or authorized person on the account.

The Company may, however, implement lesser, greater, or different requirements for business customers to whom the Company has assigned a dedicated account representative. Where the Company has implemented specific identity confirmation requirements for a business customer, those requirements will apply instead of the identity confirmation requirements contained in this Policy. All other portions of this Policy will continue to apply to such business customers.

### **BACK-UP METHOD OF CONFIRMING IDENTITY**

The Company may create a back-up method to confirm the identity of a customer or authorized person. The back-up method will require the customer to provide information that the Company will keep in the account record for this purpose. Readily available biographical information about the customer or the account cannot be used. Acceptable information includes selecting a secret question and answer that does not use readily available biographical information about the customer or the account.

The Company may request multiple pieces of information that can be used for back-up authentication of identity and may require customers and authorized persons to provide more than one piece of information when confirming identity by the back-up method.

### **CREATION OF PASSWORDS AND BACK-UPS**

The Company will create a password and backup for each new and existing customer account either by assigning a password or by allowing the customer to select a password. The Company may require customers to utilize separate passwords for on-line account access and for customer-initiated telephone calls.

A password and backup will be created for new customers at the time the customer signs up for service.

A password and backup will be created for existing customers who do not already have one. The Company may require existing customers with passwords to obtain a new password.

#### **Passwords and Back-ups Selected By Customers**

In those instances in which the customer selects a password or back-up, the following methods may be used:

1. the Company calls the customer at the served telephone number and allows the customer to select the password or back-up during the call;
2. the Company mails a temporary password to the address on the account so that the customer can call back or log-in online to select a new password after confirming his or her identity using the temporary password;
3. a new or existing customer selects a password or back-up during a visit to a business office or retail location after confirming his or her identity by providing a valid, government-issued photo identification; or
4. an existing customer with a password accesses the account using the existing password to establish a new password or back-up.

#### **Passwords and Back-ups Assigned By The Company**

In those instances in which the Company assigns a password or back-up, the Company will provide the password or back-up to the customer or authorized person only as follows:

1. the Company mails the password or back-up to the address on the account;

2. the Company calls the customer at the served telephone number; or
3. the customer or authorized person visits a business office or retail location and confirms his or her identity by providing valid, government-issued photo identification.

### **NOTICES OF ACCOUNT CHANGES**

The Company immediately will notify customers of each time that a password, back-up, or address on an account is changed, and whenever on-line access to an account is created. No such notice will be provided, however, when a customer first establishes service or a password or back-up is first created.

The notice will notify the customer that a change has occurred, but cannot state what kind of information changed (*i.e.* address, password, backup, or online account access) and cannot reveal the new information.

The Company may provide the notice by one of the following methods:

1. the Company calls the served telephone number and speaks directly with the customer or leaves a voicemail message;
2. the Company sends a text message to the served telephone number; or
3. the Company mails a notice to the address on the account (*i.e.* the address that was on the account for at least 30 days prior to the change, not the new address).

### **CUSTOMER REQUESTS FOR EXISTING PASSWORDS OR BACK-UPS**

The law prohibits the Company from providing an existing password or back-up to a customer. If the customer or authorized person loses or forgets both the password and back-up, then the Company must create a new password and back-up using the procedures applicable to an existing customer.

### **DISCLOSURES OF CPNI UPON WRITTEN CUSTOMER REQUEST**

The Company must honor written directives from a customer to disclose his or her CPNI. Disclosure of CPNI as directed in writing by the customer is not a violation of the applicable law or of this Policy as long as the identity of the customer is confirmed as required by this Policy.

## USE OF CPNI WITHOUT CUSTOMER APPROVAL

The Company cannot use, disclose, or permit access to a customer's CPNI without obtaining prior customer approval, except as follows:

### Disclosures Required by Law

No customer approval is needed to use, disclose, or permit access to CPNI as required by law. Examples include disclosures required by a court order or by laws requiring reporting of certain kinds of criminal conduct.

### Non-marketing Purposes

No customer approval is needed to use, disclose, or permit access to CPNI for the following non-marketing purposes:

- Protecting the rights or property of the Company (includes using CPNI to collect unpaid charges); and
- Protecting the Company, other carriers, and end-user customers from fraudulent, abusive, or unlawful use or subscription to service

### Marketing Purposes

No customer approval is needed to market the following services to customers:

- Inside Wire Services (installation, maintenance, repair)
- Customer Premises Equipment (sales and leasing)
- Voice mail or voice messaging
- Call answering
- Voice storage and retrieval
- Fax store and forward
- Protocol conversion
- Adjunct-to-basic services (aka vertical or enhanced features), including but not limited to:

- Computer-provided Directory Assistance
- Caller ID
- Call Waiting
- Speed Dialing

Repeat Dialing  
Call Tracing  
Call Blocking  
Call Monitoring  
Call Forwarding  
Call Tracking  
Call Return  
Centrex features

- New, additional, or improved services within the category or categories of service the customer already purchases.

EXAMPLE 1: Ms. Jones purchases local telephone service from the Company, but is presubscribed to AT&T for long distance service, and does not have Internet service. The Company may use Ms. Jones' CPNI to market new, additional, or improved local telephone services to her, but cannot use her CPNI to market long distance or Internet service to her.

EXAMPLE 2: Mr. Smith purchases a bundled service offering that includes local telephone service, long distance usage, and Internet access. The Company may use Mr. Smith's CPNI to market new, improved, or additional services to him in any or all three of these categories, either individually or on a bundled basis.

- Services within the category or categories of service the Company previously provided to a former customer.

EXAMPLE 1: Mr. Smith previously purchased local telephone service from the Company. He currently purchases local telephone service from a competitor. The Company may use his CPNI to market local telephone service to him, but cannot use his CPNI to market other services to him.

EXAMPLE 2: Ms. Doe currently purchases long distance telephone service from the Company. She has executed a Letter of Authorization to switch her service to a competitor, and the competitor has provided the LOA to the Company. Prior to processing the LOA and completing the switch, the Company cannot use her CPNI in marketing efforts designed to keep her from switching to the competitor.

### **USE OF CPNI WITH CUSTOMER APPROVAL**

The Company maintains a system by which the status of a customer's CPNI approval can be clearly established. All personnel are required to confirm whether a customer has consented to a particular use or disclosure of his or her CPNI before using, disclosing, or permitting access to his or her CPNI.

If customer consent has been obtained properly, the Company may use a customer's CPNI to market services to that customer that are in a different category of business from those the customer already purchases, and for other lawful purposes as approved by the customer.

EXAMPLE: Ms. Jones purchases local telephone service from the Company, but is presubscribed to AT&T for long distance service, and does not have Internet service. After properly obtaining consent from Ms. Jones, the Company may use Ms. Jones' CPNI to market long distance or Internet service to her.

## **OBTAINING CONSENT TO USE A CUSTOMER'S CPNI**

Customer approval may be obtained through written, oral, or electronic means.

### Methods for Obtaining Customer Approval

There are three methods for obtaining customer approval to use, disclose, or permit access to CPNI:

1. **Opt-In Method.**

Customer approval is obtained when the customer, after receiving notice, affirmatively and expressly consents to the use, disclosure, or access to his or her CPNI as described in the notice. Opt-In approval must be obtained before a customer's CPNI may be used, disclosed, or accessed for any purpose except in those few instances in which no customer approval is required or in which the use of Opt-Out or One-Time approval is permitted. Opt-In approval must be obtained before CPNI can be disclosed to or accessed by a joint venture partner or independent contractor.

2. **Opt-Out Method.**

Customer approval is assumed 30 days after written or electronic notice is given (33 days from date of mailing, if notice is mailed) unless the customer expressly denies consent. Opt-Out notices must be sent every two years. Opt-Out approval is valid only for the purpose of marketing communications-related services, (including those in a line of business different from the services the customer already purchases) by the Company, its affiliates, and its agents.

3. **One-Time Use Method.**

Oral notice may be given and oral approval may be obtained during the course of a single telephone call. Such approval is valid only for the duration of the call. The Company bears the burden of proving that oral approval was properly obtained.

### Revoking or Changing Consent

Except for oral, one-time-use approval, customer approval or disapproval remains in effect until the customer revokes or changes such approval or disapproval.

The Company maintains a free 24-hour per day, 7-day per week method for customers to give, revoke, or change their approval for the use and disclosure of CPNI.

### Notification Requirements

Prior to any solicitation or request for customer approval, the Company must notify the customer through oral, written, or electronic means, that the customer has the right to restrict the use of, disclosure of, and access to the customer's CPNI. The solicitation must be proximate in time to the notification of a customer's CPNI rights. If a written solicitation is mailed to a customer, a notice of the customer's CPNI rights must be included in the same envelope.

If any notification is translated into another language, then all portions of the notification must be translated into that language.

### Contents of Notification

The notification must provide sufficient information to enable the customer to make an informed decision about whether to permit the Company to use, disclose, or permit access to the customer's CPNI. The notification must:

- Specify the types of information that constitute CPNI, describe the purposes for which CPNI will be used, and inform the customer of the right to disapprove of those uses, and to deny or withdraw access to CPNI at any time;
- State that the customer has a legal right, and the Company has a legal duty, to protect the confidentiality of CPNI;
- Advise the customer of the precise steps necessary to grant or to deny access to CPNI, and must clearly state that a denial of approval will not affect the provision of any services to which the customer subscribes; and
- State that any approval or denial of approval for the use of CPNI for lines of business other than those to which the customer currently subscribes will stay in effect until the customer affirmatively revokes or limits such approval or denial.

Further, the notification must be comprehensible and not be misleading. If written notification is provided, the notice must be legible and be placed in an area so as to be readily apparent to a customer.

The notification may state that the customer's approval to use customer-specific CPNI might enhance the Company's ability to offer products and services tailored to the customer's needs. It also may state that the Company must disclose CPNI to any person upon written request of the customer.

The notification may not include any statement attempting to encourage a customer to freeze third party access to customer-specific CPNI.

#### Special Rules for Obtaining Oral, One-Time Use Approval

Oral approval to use CPNI one time and only for the duration of the call, regardless of whether the call was originated by the customer or by the Company, can be obtained only after the customer's identity has been confirmed and appropriate notice is provided to the customer. Oral notice is acceptable.

The oral notice must comply with the general notice requirements, except that the Company need not advise the customer:

- that the oral, one-time approval does not alter any prior opt-out elections made by the customer;
- that CPNI will be disclosed to affiliates or third-parties, unless the one-time use of CPNI will result in disclosure of CPNI to affiliates or to third parties;
- of the method for altering or withdrawing approval to use, disclose, or permit access to CPNI in the future as long as it is clear that the oral, one-time approval is valid only for the duration of the call; and
- of the steps necessary to grant or to deny approval to use, disclose, or permit access to CPNI as long as it is clear that the Customer can deny access to CPNI for purposes of the current call.

#### Special Rules for Obtaining Customer Approval by Electronic Mail

Before using electronic mail to obtain customer approval to use, disclose, or permit access to CPNI, the Company must:

- obtain prior, verifiable approval from the customer to communicate with the customer via electronic mail with respect to their service generally or with respect to CPNI particularly;
- state clearly in the subject line of the electronic mail message that the message is a request for approval to use, disclose, or permit access to CPNI;

- permit customers to reply directly to all electronic mail messages soliciting approval to use, disclose, or permit access to CPNI, *i.e.* send-only electronic mail addresses cannot be used to send CPNI notices and the electronic mail address used to send solicitations must be monitored for replies and for delivery error messages; and
- not rely upon undeliverable electronic mail messages for customer approval to use, disclose, or permit access to CPNI (another form of notification must be used).

### **ADDITIONAL SAFEGUARDS: CONTRACTORS AND JOINT VENTURERS**

The Company may disclose CPNI to independent contractors and joint venturers, or may permit them to access CPNI, for purposes of marketing or providing communications–related services only after obtaining opt-in approval from each customer whose CPNI will be disclosed.

All independent contractors and joint venturers must abide by the applicable law and rules. At a minimum, each contractor and joint venturer must enter a confidentiality agreement.

Each independent contractor and joint venturer is:

- required to use CPNI only for the purpose of marketing or providing the service for which the CPNI was disclosed to them;
- prohibited from using, disclosing, or permitting access to CPNI to anyone else, unless required to do so by law, such as by court order; and
- required to implement policies, procedures, and safeguards to ensure ongoing confidentiality of CPNI, including identity confirmation requirements.

### **ADDITIONAL SAFEGUARDS: HACKING AND PRETEXTING**

The Company may utilize additional means of safeguarding CPNI from hacking and other unauthorized electronic intrusion. Among other things, the Company may encrypt CPNI, may track individual employee access to CPNI, and may utilize software and other means to detect and to prevent unauthorized access to CPNI through electronic means.

The Company will take reasonable measures to discover and to protect against pretexting. Company personnel who directly interact with customers, especially customer service representatives, play a critical role in identifying pretexting and in preventing unauthorized disclosure of CPNI.

Company personnel who reasonably believe that a person is engaged in pretexting should tactfully and respectfully end the communication. Company personnel also must report incidents of pretexting and unauthorized access to or disclosure of CPNI.

### **AGGREGATE CUSTOMER INFORMATION**

The Company may compile and use aggregate customer information for marketing purposes, and it may disclose such information to affiliates, contractors, joint venturers, or third-parties. Aggregate customer information is not subject to the same restrictions as apply to CPNI.

All aggregate customer information so compiled and used must be provided to third-parties who request it, including competitors. Third-parties who request such information, however, must identify the scope and type of the information requested. The Company must provide the information to the requesting third-party at the same rates and on the same terms as it provides the information to itself.

### **SUBSCRIBER LIST INFORMATION**

The Company must provide subscriber list information to third parties who request it for the purpose of publishing directories in any format. The information must be provided on a timely and unbundled basis, and under terms and conditions that are nondiscriminatory and reasonable.

Subscriber list information will be maintained separately from CPNI within the customer account record system. Company personnel are prohibited from accessing, using, or disclosing CPNI as a substitute method of accessing, using, or disclosing subscriber list information.

### **RECORD-KEEPING REQUIREMENTS**

The Company will maintain the following records for the time period specified.

#### **Records of Breaches**

The Company will maintain records of each breach for at least two years following discovery of each breach. If it is available, the Company will maintain records of the following:

- Date breach was discovered;
- Date breach was reported to law enforcement officials;

- Date breach was reported to customers or to the public;
- Detailed description of the CPNI that was the subject of the breach;
- The circumstances and other known details of the breach, such as how the breach occurred;

If it is available, the Company will strive to maintain records or copies of the following:

- The Company's reports to law enforcement and regulatory agencies;
- Communications between the Company, law enforcement officials and regulatory agencies, such as correspondence, notes of telephone calls, and electronic mail messages;
- Notices provided to customers and to the public;
- Reports generated by law enforcement officials and regulatory agencies; and
- Reports, summaries, and analysis generated by the Company or on behalf of the Company, such as by consultants or private investigators.

#### Customer-approval Records

The Company will maintain for at least one year records of customer approvals – whether oral, written, or electronic – for use, disclosure, or permitting access to individual CPNI.

#### Sales and Marketing Campaign Records

The Company will maintain for at least one year records of each sales and marketing campaign that uses CPNI. For each campaign, the records are to include a description of the campaign, the specific CPNI that was used in the campaign, the date and purpose of the campaign, and what products or services were offered as part of the campaign.

### **REPORTING REQUIREMENTS**

The Company will prepare and file, as necessary, the following reports:

#### Annual Compliance Certificate

The Company will prepare an Annual Compliance Certificate for the preceding calendar year.

The Annual Compliance Certificate, on or before March 1 of each year, will be filed as follows:

- Filed with the FCC in EB Docket No. 06-36; and
- Filed in the Company's public file and made publicly available at the Company's central business office for inspection and copying during regular business hours.

The Annual Compliance Certificate must include the following:

- Signature of an officer with personal knowledge of the facts stated;
- Statement that the operating procedures established by the Company and in use during the preceding calendar year are adequate to ensure compliance with the FCC's CPNI rules;
- Explanation of how the Company's procedures ensured such compliance during the preceding calendar year;
- Explanation of any actions taken against data brokers during the preceding calendar year;
- Summary of customer complaints received by the Company during the preceding calendar year regarding unauthorized disclosure of CPNI.

#### Security Breach Reports

The Company will report each breach it discovers as soon as practicable, but not more than seven (7) business days after reasonably discovering that a breach has occurred. The Security Breach Report will be filed electronically with the United States Secret Service and the Federal Bureau of Investigation via the FCC's website at [www.fcc.gov/eb/cpni](http://www.fcc.gov/eb/cpni).

Except as required by federal law or as permitted by this Policy, the Company WILL NOT notify customers or the public of a breach until at least the eighth business day after the filing of a Security Breach Report. After consulting with the investigating law enforcement agency, the Company may notify customers and the public within the first seven business day following the filing of a Security Breach Report only if the Company believes that there is an extraordinarily urgent need to notify a customer or class of customers in order to avoid immediate and irreparable harm.

On or after the eighth business day following the filing of a Security Breach Report, the Company will notify customers and the public of the breach unless:

1. the investigating law enforcement agency determines that such notice would impede or compromise a criminal investigation of the breach or would harm national security; and
2. the investigating law enforcement agency in writing directs the Company not to issue such a notice for an initial period of up to 30 days or for any subsequent period of time deemed reasonably necessary by the investigating law enforcement agency.

The investigating law enforcement agency may rescind such a directive by informing the Company in writing that notice to customers or to the public would no longer impede or compromise a criminal investigation or would no longer harm national security.

The contents of the notice to customers and to the public of breaches can be tailored to the specifics of each situation.

### Opt-out Failure Reports

The Company will notify the FCC in writing whenever the opt-out mechanism does not work properly and the error is more than an anomaly. The report will include a description of the opt-out mechanism used, the problem, the proposed remedy, and the timeframe for implementing the remedy. The report also will include a copy of any notice provided to customers, contact information for the Company, and a statement of whether the incident has been reported to the state commission and the action, if any, taken by the state commission.

### **BILLING NAME AND ADDRESS**

In addition to being protected as CPNI, Billing Name and Address information is subject to additional protection under federal law. The following requirements apply to BNA in addition to the CPNI rules.

### Use and Disclosure of BNA

A customer's BNA may be disclosed only to other telecommunications service providers who provide service to the customer or to authorized billing and collection agents for the purpose of billing and collecting charges for telecommunications service.

The Company and anyone to whom it discloses BNA may use BNA only:

- to bill and collect amounts due for telecommunications services provided by the billing party;
- to provide equal access; and

- to verify orders for new service, to identify customers who have moved, to prevent fraud, and similar non-marketing purposes.

#### Customer Notice

The Company must notify customers that BNA will be disclosed, “pursuant to Policies and Rules Concerning Local Exchange Carrier Validation and Billing Information for Joint Use Calling Cards, CC Docket No. 91-115, FCC 93-254, adopted May 13, 1993”:

- whenever the customer uses a joint use calling card to pay for services obtained from the Company; and
- whenever the customer accepts a third-party call or a collect call.

The Company must notify customers who have unlisted or unpublished telephone numbers that:

- Customers have a right to prevent disclosure of their BNA for third-party, collect, and calling card calls; and
- Customers are deemed to have consented to disclosure of their BNA unless they affirmatively request that their BNA not be disclosed within 30 days of receiving the notice.

The Company must not disclose BNA for third-party, collect, and calling card calls if the customer has requested that their BNA not be disclosed.

#### **TRAINING AND SUPERVISION**

All appropriate personnel will be trained in the use, disclosure, and access to CPNI and BNA. Access to CPNI and BNA will be limited to personnel who have completed training and whose duties require such access.

The Company will utilize a supervisory review process to ensure compliance with CPNI and BNA policies and procedures. All outbound marketing efforts that use CPNI must be approved in advance by the officer having responsibility for marketing.

#### **VIOLATIONS**

All Company personnel are required to comply with the CPNI and BNA policies and procedures. Violations will result in appropriate disciplinary action, up to and including termination.