MASSENA
TELEPHONE COMPANY

Customer Proprietary Network Information

Company Procedures

CPNI

Table of Contents

I. General Statement of Corporate Policy

II. CPNI Shared Among Affiliated Companies

III. Protection of Carrier Information

IV. Acceptable Uses of CPNI

V. Customer Access to Online Accounts

VI. Customer Notification of Account Changes and Breaches

VII. Recordkeeping

VIII. Employee Training and Discipline

IX. Security of CPNI Data

X. Annual CPNI Certification

XI. Definitions

I. General Statement of Corporate Policy

It is the policy of The Company to adhere to the legal requirements set forth in 47 U.S.C. §222 of the Communications Act and the FCC Rules set forth in 47 C.F.R. §64.2001 through 64.2011 (the "CPNI Rules"). Each employee of The Company who has access to CPNI will be aware of the rules and safeguards in place. If any circumstances arise where an employee of The Company is unsure of how to apply the rules, they should bring the issue to the CPNI Compliance Officer. Where a gray area exists, The Company will **always** err on the side of caution in order to safeguard CPNI.

The Company will only grant access to CPNI to employees who need access and those employees should not use, disclose, or permit access to CPNI except as permitted in The Company procedures.

The following pages of this manual state in more detail how The Company plans to adhere with the CPNI Rules. Each employee is expected to read and comprehend the manual in its entirety. If clarification needs to be made on any section of the manual, the employee should bring it up with the CPNI Compliance Officer.

II. CPNI Shared Among Affiliated Companies

The Company does not have any Affiliated Companies. CPNI will only be accessed and used in accordance with this document by The Company and its employees.

III. Protection of Carrier Information

The Company will only use proprietary information received from another carrier for its intended purpose and as permitted or required by applicable law. For example, The Company will never use information from another carrier for its own marketing when it was intended for provisioning telecommunications services.

IV. Acceptable Uses of CPNI

The FCC has allowed companies to treat call detail and non-call detail CPNI differently; however, it will be The Company's policy to apply call-detail safeguards to all forms of CPNI *except as explicitly stated otherwise in this section.*

Employees may use, disclose, or permit access to CPNI in the following situations.

A. General Uses of CPNI Without Prior Customer Approval

The Company will comply with legitimate requests made by law enforcement for CPNI. Employees who receive these requests should immediately notify the CPNI Compliance Officer. It is the CPNI Compliance Officer's responsibility to seek legal counsel (if needed) and respond to the request.

The Company may use, disclose, or permit access to CPNI directly or indirectly through its agents to -

- Initiate, render, bill, and collect for telecommunications services.
- Protect the rights or property of the carrier, or to protect the users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.
- Provision inside wiring installation, maintenance, and repair services.
- Conduct research on the health effects of CMRS.
- Provide call location information concerning the user of a commercial mobile service -
    - To a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services.
    - To inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm.
    - To providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

Any questions that arise with one of the points above should be brought to the CPNI Compliance Officer.

IV. Acceptable Uses of CPNI (cont.)

B. Customer Requests for CPNI

When an employee receives a request from the customer for their CPNI, the employee should determine how the request was made (phone, email, in person) and then follow the proper procedures detailed below in order to complete the customer's request in compliance with the CPNI Rules. If the employee has any questions about how to handle a request for CPNI, they should bring that question to the CPNI Compliance Officer.

1. Customer Initiated Telephone Requests for CPNI

When a customer makes a request or has a question over the phone regarding CPNI, The Company will only provide the information through one of the two methods listed below. It will be up to the customer which option they would like The Company to use.

If the customer is able to provide the CPNI in question without any assistance, The Company can proceed without authenticating the customer. However, if any additional information is needed in order to assist the customer and the customer cannot provide that information (or the customer could not initially provide all the needed information), then The Company must authenticate the customer and respond to their request through one of the two methods listed below.

- The Company may send the information requested to the customer's "address of record." The "address of record" could be either the mailing address of record or a pre-established electronic address of record which has been associated with the customer's account for at least thirty (30) days.

- The Company may call the customer back at their "telephone number of record." The "telephone number of record" is the telephone number associated with the customer's underlying service and **not** an alternative number designated as a customer's "contact information."

If the customer requests call detail CPNI, the employee should complete a "Call Detail Request Form" (found in The Company's CPNI binder) and use one of the methods above to complete the request. The Company will not provide CPNI to a designated person unless the customer submits a written request and The Company follows its procedures set forth in section IV.B.3.

IV. Acceptable Uses of CPNI (cont.)

B. Customer Requests for CPNI (cont.)

2. Carrier Retail Location Requests for CPNI

When a customer makes a request for CPNI at The Company's retail location, The Company will request to see a government-issued photo ID (driver's license, passport, etc.) that is not expired. The ID must match the name listed on the account or someone listed as an authorized user on the account.

One exception will be made for customers who request the amount of their bill for the purpose of paying their bill. In this case, The Company will disclose the amount due or amount past due but will not disclose whether the account is current, or past due, so as not to inadvertently reveal monthly amount spent.

If the customer requests CPNI at The Company's retail location, the employee should ask the customer to complete a "CPNI Request Form" (found in The Company's CPNI Manual) and follow the procedures set forth in section IV.B.3.

If the customer is able to provide the CPNI in question without any assistance, The Company can proceed without authenticating the customer. However, if any additional information is needed in order to assist the customer and the customer cannot provide that information (or the customer could not initially provide all the needed information), then The Company must authenticate the customer and respond to their request after the customer produces a valid photo ID. The customer would have the option to request the information be sent to their postal or electronic "address of record" if they did not have a photo ID with them.

IV. Acceptable Uses of CPNI (cont.)

B. Customer Requests for CPNI (cont.)

3. Written Requests for CPNI

When the customer submits a valid written request for disclosure of their CPNI, The Company will provide the CPNI to the person designated on the request form. Customers should be encouraged to make all written requests via the "CPNI Request Form" found in the CPNI Manual. An employee should honor a written request in any other form if approved by the CPNI Compliance Officer.

If the customer or authorized user on the account is requesting information for their own use, The Company will either send the information to their mailing or electronic address of record or provide the information in person after a valid ID is presented. If the customer or authorized user on the account wants The Company to disclose their CPNI to a designated person, we will first verify the request with a phone call to the telephone number of record, send a verification letter to the customer's mailing or electronic address of record, or the customer may present a valid ID at our retail location. If the request is confirmed, we will provide the CPNI to the designated person.

IV. Acceptable Uses of CPNI (cont.)

B. Customer Requests for CPNI (cont.)

4. Business Customer Exceptions

The Company may choose to utilize contracts with certain business customers that will dictate how a specific business's CPNI is protected. These contracts will assign a dedicated account representative which the business customer will be able to reach directly as their primary contact. The contract will also include other specific CPNI safeguards negotiated by the business customer and The Company. The Company's CPNI Compliance Officer should always be included in the negotiation process.

IV. Acceptable Uses of CPNI (cont.)

C. Marketing

All out-bound marketing campaigns will be approved and reviewed by the CPNI Compliance Officer for compliance with the CPNI Rules, and The Company will use the "Marketing Campaign Assessment Form" to document this process. If the CPNI Compliance Officer has any uncertainty about the marketing campaign, they should seek counsel from their consultant or legal advisor. Marketing campaigns not using CPNI do not fall under the CPNI Rules; however, The Company will review all marketing campaigns to further safeguard CPNI. Employees should bring any and all questions related to marketing to the CPNI Compliance Officer. The Company will not use CPNI in its marketing efforts except as listed below.

1. Customer Permission Not Required

The Company is not required to obtain permission from the customer in the following scenarios:

a) **In-Bound Marketing:**

When the customer initiates the communication and The Company does not need to use CPNI in order to answer a marketing related question, no customer permission is required.

b) **Out-Bound Marketing**

- The Company may send marketing documents to its customers as a whole or on an aggregate level within a service category without the approval of the customer. Marketing in this manner does not use CPNI because all customer specific information has been stripped away.

- The Company may send marketing documents to its customers based on their subscriber list information. For example, this may include targeting customers based on their address. Customers who have unpublished numbers will not be included in these types of marketing efforts. Marketing in this manner does not use CPNI since it is based on public information.

IV. Acceptable Uses of CPNI (cont.)

C. Marketing (cont.)

1. Customer Permission Not Required (cont.)

b) **Out-Bound Marketing (cont.)**

- The Company may use CPNI to market to its customer the same service from which the CPNI was taken. For example, The Company may use CPNI to market a new long distance plan to a customer who already subscribes to The Company's long distance service. If the customer subscribes to multiple categories of service, The Company may use their CPNI to market different packages of **only** the existing services. For example, if the customer already subscribes to local telephone and internet service, The Company may use CPNI to market different packages of those two services to the customer.

- The Company may use CPNI to market adjunct-to-basic (complement) services to the customer based on the underlying service the customer already receives. For example if the customer receives local telephone service, The Company may use CPNI to market Caller ID, Call Waiting, 3-Way Calling, Call Forwarding, etc. to the customer.

IV. Acceptable Uses of CPNI (cont.)

C. Marketing (cont.)

2. Customer Permission Required

The Company is required to obtain permission from the customer in the following scenarios:

a) **In-Bound Marketing:** When the customer initiates the communication, The Company may use his/her CPNI for the duration of their interaction only with the customer's permission to do so. (If the customer's original purpose for contacting The Company is marketing related no permission is needed.) If permission is needed, The Company will tell the customer what CPNI is, that The Company has the duty to protect it, that it will only be used for the duration of this interaction, and why they need access to it.

If the intent of the customer's contact was not marketing related and if The Company does **not** need to disclose any CPNI to the customer, they only need to ask for permission to access the customer's CPNI.

If The Company does need to disclose CPNI to the customer, The Company should first authenticate the customer before disclosing any CPNI. The Company may authenticate the customer with the methods described in Section IV.B.1. & IV.B.2. If the intent of the customer's contact was not marketing related and the customer is authenticated, The Company then needs to ask for permission to access the customer's CPNI. The Company may then disclose CPNI to the customer for the purpose of marketing services to the customer. If call detail CPNI is disclosed, the employee should complete a "Call Detail Request Form" (found in The Company's CPNI Manual).

b) **Out-Bound Marketing:** The Company does not use CPNI in marketing campaigns and employees are prohibited from accessing CPNI for marketing purposes except as described in Section IV.C.1.

V. Customer Access to Online Accounts

The Company will require passwords for all customers who want and/or have access to their CPNI via online accounts.

A. New Customers

New customers will establish passwords and answers to the back-up question at the time service is initiated.

B. Existing Customers

Existing customers will first be authenticated without the use of "readily available biographical information" and "account information" and then establish a password and an answer to the back-up question. The customer will be authenticated and establish their password in any of three ways:

1. The Company may send a form to the customer's address of record. The customer will be responsible for completing the form (which will include picking a password) and sending it back to The Company, so that, The Company can establish the customer-set password.

2. The Company may send a document which will include a PIN to the customer's address of record. The customer will either use this PIN to login to their online account and then establish a password or call The Company, tell the employee the PIN, and then establish a password.

3. The customer may establish a password at The Company's retail location if the customer provides a valid ID.

The customer will be prompted or reminded by The Company to select an answer to the back-up question the first time they login to their online account. In every option listed above, The Company will remind customers that it is best not to use readily available biographical information and account information when establishing a password.

The Company will not require existing customers to re-establish their password; however, The Company will remind them not to base their password on readily available biographical information or account information.

If The Company has access to their customers' passwords and answers to back-up questions, those records will be in a secure file and employee access will be limited to those who need access.

VI. Customer Notification of Account Changes and Breaches

The Company will notify customers of all applicable account changes and breaches to their CPNI as detailed below. Any questions regarding these two issues should be brought to the CPNI Compliance Officer.

A. Account Changes

The Company will notify an existing customer immediately if a password, customer response to a back-up question, online account, or address of record is created or changed. The Company will not notify a customer of these changes when he/she initiates service. All notices will only inform the customer that a change was made and will not include any specific information regarding the change such as the new address, new password, or answer to the back-up question. The Company may notify the customer of the change in any one of the following ways:

- The Company may send a letter to the customer's address of record.
- The Company may send a letter to the customer's electronic address of record. The Company will only send this information to the electronic address of record if the customer has established this address and it has been on file for at least thirty (30) days, and the customer has given express, verifiable approval to send notices via email.
- The Company may leave a voicemail at the customer's telephone number of record.

B. Customer CPNI Breaches

The Company will take all preventive measures in order to protect customers' CPNI; however, if The Company can reasonably determine that a breach of a customer's CPNI has occurred, The Company will alert law enforcement by sending electronic notification through the designated central reporting facility – http://www.fcc.gov/eb/CPNI. The Company will adhere to the following timetable set by the FCC when reporting these breaches.

- The Company will report breaches to the central reporting facility within seven (7) business days of reasonably determining a breach has occurred.
- The Company will notify the customer that a breach to their CPNI has occurred no earlier than seven (7) full business days after notifying law enforcement.

VI. Customer Notification of Account Changes and Breaches (cont.)

B. Customer CPNI Breaches (cont.)

- Law enforcement may request that The Company wait longer than seven (7) full business days if they feel that customer notification would impede the investigation.

- The Company may, if it feels necessary, **request** to notify the customer earlier than seven (7) full business days after notifying law enforcement. The relevant investigating authority must grant this request before The Company may notify the customer.

Employees should immediately notify the CPNI Compliance Officer if they have any reason to believe a breach has occurred. The CPNI Compliance Officer should seek legal counsel in the event of a breach.

VII. Recordkeeping

The Company recognizes that the FCC has placed the burden of proof on them in all CPNI discrepancies. The Company also recognizes that there are specific CPNI rules in place regarding minimum retention periods for various documents such as Opt-Out agreements, marketing campaigns and customer complaints. The Company will maintain a list of documents and their retention periods in the CPNI Manual which mirror FCC rules and will retain documents in accordance to that list. All records will be stored in a manner that complies with Section XIII. Any questions regarding this section should be brought to the CPNI Compliance Officer.

VIII. Employee Training and Discipline

The FCC requires that every company train their personnel on CPNI and also create an express disciplinary process for employees who fail to adhere to the CPNI Rules.

A. Employee Training

All employees will be trained as to when they are and are not authorized to use CPNI. The amount of training an employee receives may depend on their access level and use of CPNI on a daily basis. All training questions should be brought to the CPNI Compliance Officer. The following are the forms of training that will be made available to the various employees of The Company.

- Employees will be required to read The Company's CPNI Procedures document. The employee will sign that he/she has read and understands the policies that are in place and is able to comply with those procedures. The signed documentation will be kept in The Company's CPNI Manual.

- The Company will have CPNI updates at least once a year or when new rules become proposed or effective in order to keep affected employees up-to-date. Documentation of these updates will be kept in The Company's CPNI Manual.

- *The Company has made or may make a third party training session available to its employees during which employees can be trained on CPNI. Documentation of third party training sessions will be kept in The Company's CPNI Manual.*

B. Employee Discipline

The Company will discipline the employee when he/she fails to adhere to The Company's CPNI procedures and the measure of discipline taken will depend on the level of CPNI misuse. Employee discipline measures will include any reasonable discipline actions, in accordance to normal Company policy, up to and including employee termination.

IX. Security of CPNI Data

The Company will take reasonable measures to discover and protect against activity that is indicative of pretexting, and in any instance where an employee feels that a CPNI file may have been misused or a breach may have occurred, they should immediately notify the CPNI Compliance Officer.

The Company recognizes that the security of their files containing CPNI is of the utmost importance. Employees who have access to CPNI whether on the computer or through paper files are to practice extreme caution when accessing and using that information. The Company will protect CPNI data in the following ways.

A. Electronic Files

- Files and electronic databases will not be stored or used on any public network.
- Files and electronic databases will always be protected by a password.
- Only employees who need access to the electronic files and databases will be granted access to that information.

B. Paper Files

- All paper files containing CPNI will be kept in a locked filing cabinet or some other locked storage device or facility.
- Only employees who need access to the paper files will be granted access to that information.

X. Annual CPNI Certification

The Company will file on an annual basis a compliance certificate and accompanying statement in accordance with 47 C.F.R. §64.2009(e). Along with the filing, The Company will include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. The certificate will be signed by the CPNI Compliance Officer of The Company and filed by March 1st every year starting in 2008. All filings that have been made with the FCC will be kept in The Company's CPNI Manual.

XI. Definitions

Account Information:

Information that is specifically connected to the customer's service relationship with the carrier, including such things as an account number or any component thereof, the telephone number associated with the account, or the bill's amount.

Address of Record:

The address that the carrier has associated with the customer's account. The address must be on file for at least thirty (30) days.

Affiliate:

An entity/person that (directly or indirectly) owns or controls, is owned or controlled by, or is under common ownership or control with, another entity/person. The term "own" means to own an equity interest (or the equivalent thereof) of more than 10 percent.

Breach:

Occurs when a person, without authorization or exceeding authorization, has intentionally gained access to, used or disclosed CPNI.

Call Detail:

Includes any information that pertains to the transmission of specific telephone calls including, the number called or where the call came from, and the time, location, or duration of any call.

CPNI:

Account Information Call Detail and other non-public, personally identifiable information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications services subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. Examples: Sensitive personal information; phone numbers called; time, date and duration of calls; how much a customer spends monthly; type of network a consumer subscribes to; calling patterns; optional services used; frequently called states, numbers, etc.; and for business customers it could include line size.

Electronic Address of Record:

The electronic address (email) the carrier has associated with the customer's account. The address must be on file for at least thirty (30) days and the customer must have given express, verifiable approval to send notices via email.

Non-Call Detail:

Any CPNI which does not fall under the category of call detail. Examples would be: remaining minutes of use, call forwarding, call waiting, billed amount, other information relating to the customers account.

Readily Available Biographical Information:

Includes such things as the customer's social security number, or the last four digits of that number; the customer's mother's maiden name; a home address; or a date of birth.

Subscriber List Information:

Any information (a) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (b) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

Telephone Number of Record:

The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

Valid Photo ID:

A government-issued personal identification with a photograph such as a current driver's license, passport, or comparable ID that is not expired.