



CPNI (Customer Proprietary Network Information)

Regulatory Requirement: As a telecommunications carrier, FiberNet Monticello (FNM) is subject to certain requirements governing the use or disclosure of Customer Proprietary Network Information (CPNI). The CPNI statutory and regulatory requirements are largely consumer protection provisions, which set forth the circumstances under which FNM may use, disclose or permit access to CPNI with and without the customer's approval. FNM will supplement these policies and procedures as necessary and appropriate to ensure compliance with the FCC's regulatory requirements. In all markets where the Company provides telecommunications services, FNM has a duty to protect the proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers and customers, including telecommunications carriers reselling FNM's telecommunications services. When FNM receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service, FNM will use such proprietary information only for such purpose, and shall not use such proprietary information for its own marketing efforts. Except as required by law or with the approval of the customer, FNM shall only use, disclose or permit access to individually identifiable CPNI that it receives or obtains by virtue of its provision of a telecommunications service for purposes of providing (1) the telecommunications service from which such information is derived, or (2) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories. FNM shall also disclose CPNI, upon the affirmative written request by the customer, to any person designated by the customer.

FNM is permitted to use, disclose or permit access to CPNI obtained from its customers, either directly or indirectly through its agents, in the following circumstances:

- (1) To initiate, render, bill and collect for telecommunications services;
- (2) To protect the rights or property of FNM, or to protect users of FNM's telecommunications services and other carriers from fraudulent, abusive or unlawful use of, or subscription to, such services; and
- (3) To provide any inbound telemarketing, referral or administrative services to the customer for the direction of the call, if the customer and the customer initiated such call approves of the use of such information to provide such service.

Purpose: This Policy and Procedure documents the operating procedures FNM will undertake to satisfy these regulatory requirements.

Scope: All markets in which FNM provides telecommunications services.

I. INTRODUCTION

This document contains FNM's policies and procedures for complying with the obligation to protect the confidentiality of its telecommunications customers consistent with applicable law, including the FCC's regulations governing CPNI. All FNM employees are required to understand and comply with the policies and procedures. Note that information that is not CPNI may nonetheless be entitled to legal protection for reasons separate and apart from the FCC's regulations. Questions concerning the permissible use of CPNI and other customer information without customer approval should be directed to the Wholesale Markets & Video Content Manager.

II. DEFINITION OF CPNI

1. CPNI is information FNM obtains or creates in the normal course of providing local or long distance telecommunications services to its customers. This information includes the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by a customer, and that is made available to FNM solely by virtue of our carrier-customer relationship.
2. CPNI also includes information contained in the bills pertaining to local and long distance service received by FNM's customers.

3. CPNI does not include the customer's telephone number, name and address since this information is typically published in a telephone directory.

4. CPNI will generally be maintained in the customer's billing records as part of the Company's billing system. The only FNM employees authorized to access the CPNI in the billing system include representatives of Senior Management, Customer Service, Broadband Service Center, Network Operations, HBC Finance Department and the CPNI Integrator. Sales and Marketing employees are not authorized to directly access CPNI from the Company's billing system, but must submit any request for customer information to the General Manager.

III. USE OF CPNI WITHOUT CUSTOMER APPROVAL

1. FNM and its authorized employees may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service to which the customer already subscribes from FNM without customer approval. FNM presently offers local and interexchange (long distance) telecommunications services.

a. If a customer subscribes to any of FNM's local and long distance services, the Company may use the customer's CPNI in the administration and provisioning of their services.

2. FNM and its employees are not permitted to use, disclose or permit access to a customer's CPNI to market additional service offerings that are not within the category of service to which the customer has already subscribed to from FNM, unless FNM has the customer's approval to do so or except as described in Section III (4) below.

a. For purposes of this provision, FNM follows the "total service approach," which allows the Company to use a customer's entire record derived from the complete services subscribed to from FNM to market improved services within the parameters of the existing carrier-customer relationship. FNM may use CPNI to market offerings related to the customer's existing telecommunications service to which the customer presently subscribes. This applies to the customer's total telecommunications subscription and is not applied on a line-by-line basis in the case of a customer who subscribes to multiple lines.

b. FNM and its authorized employees may use CPNI from short-haul toll service to market its local services only if FNM is already providing local service to the customer. FNM may not use short-haul toll CPNI to market interLATA long distance services to the customer.

c. FNM and its authorized employees may use, disclose or permit access to CPNI, without customer approval, for purposes of marketing customer premises equipment (CPE) and the following information services: voicemail or messaging services, call answering, voice storage and retrieval services and fax storage and retrieval services. Information services do not include FNM's Internet access services for this purpose.

3. FNM and its authorized employees may not under any circumstances use, disclose or permit access to a customer's CPNI to identify or track customers that call competing service providers. For example, FNM will not use local service CPNI to identify or track customers that call TDS or another local service competitor.

4. FNM and its authorized employees may properly use, disclose or permit access to CPNI, without customer approval, in the following circumstances:

a. FNM may use, disclose or permit access to CPNI in its provision of inside wiring, installation, maintenance and repair services.

b. FNM may use, disclose or permit access to CPNI for the purpose of conducting research on the health effects of commercial mobile radio services (CMRS).

c. FNM may use CPNI to market services formerly known as adjunct-to-basic services, including but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding and certain Centrex features.

5. FNM and its authorized employees may use, disclose or permit access to CPNI to protect FNM's rights or property, or to protect its users and other carriers from fraudulent, or lawful use of, or subscription to, the Company's services.

6. Any questions concerning the permissible use of CPNI without customer approval should be directed to the Video Content Manager.

IV. APPROVAL REQUIRED FOR USE OF CPNI

1. The Company's policies require that FNM obtain customer approval in either written, oral or electronic methods in accor-

dance with FCC rules allowing the use of a customer's individually identifiable CPNI information for the purpose of marketing additional communications-related services to them outside of the customer's total service relationship with the Company.

- a. It is the Company's responsibility to demonstrate or give proof that such approval has been granted by the customer. All customers will be given notice of the CPNI rights to restrict use of, disclosure of and access to that customer's CPNI, as more fully described in Section V, before any solicitation for approval.
- b. Where oral approval is obtained, the FNM representative receiving such approval must document the customer's consent by noting the date and time of the conversation and delivering a copy of such not to the CPNI Integrator. Where possible, the FNM representative should attempt to obtain written confirmation of consent from the customer.
- c. Where written approval is obtained, the FNM representative must deliver a copy of the approval form to the CPNI Integrator.
- d. The customer's decision to approve, limit or refuse the use of their CPNI information will remain in effect until such time the customer notifies FNM in either oral, written or electronic method of a change.

2. The Company will maintain records of customer notification and approval, whether oral, written or electronic, for at least one (1) year. A customer's approval or refusal and the date which this occurred can be viewed within the billing system by authorized FNM personnel, including representatives of Senior Management, Customer Service, Broadband Service Center, Network Operations, Finance Department and the CPNI Integrator. Non-authorized FNM personnel can verify a customer's CPNI status by checking with Customer Service. The CPNI Integrator will be responsible to maintain all records of notification and approvals.

3. Except for use, disclosure of and access to CPNI that is permitted without customer approval as described in Section III, or as otherwise allowed by applicable law, FNM will only use, disclose or permit access to a customer's individually identified CPNI subject to an "opt-out" approval method to obtain customer permission for marketing communication related services (including FNM's Internet access services) to that customer outside of the customer's total service relationship with the Company. This approval will extend to our agents, contractors or other companies, which perform services on our behalf. We require them to protect a customer's CPNI as required by law. FNM does not disclose an CPNI to any unaffiliated third parties for use in their own marketing. All other use, disclosure and access to CPNI requires opt-in approval.

4. Before disclosing or providing access to CPNI to any joint venture partners or independent contractors, FNM personnel must confirm that the Company has entered into an appropriate confidentiality agreement with the independent contractor or joint venture partner. Contact the Vice President of Finance or President & CEO to confirm. Any confidentiality agreement between FNM and an independent contractor or joint venture partner will include, at a minimum, the following requirements:

- a. Require the independent contractor or joint venture partner to use the CPNI only for the purpose of marketing or providing services for which the CPNI has been provided;
- b. Prohibit the independent contractor or joint venture partner from using, allowing access to or disclosing the CPNI to any other party, unless required to make such disclosure under force of law; and
- c. Require the independent contractor or joint venture partner to have appropriate protections in place to ensure the ongoing confidentiality of the customer's CPNI.
- d. Should an independent contractor or joint venture partner be used for the purpose of marketing FNM telecommunications services not within FNM's total services to that customer, customer opt-in approval is required.

V. NOTICE REQUIRED FOR USE OF CPNI

1. The Company will provide each customer with notice of the customer's right to restrict FNM's use of, disclosure of and access to their CPNI information. The Notice will also be posted on the Company's website.

- a. The Company will obtain customer approval through written notification and "opt-out" approval, which will be mailed to all existing FNM telephone customers in March of every even-numbered year. New customers will receive written notification of their CPNI rights as part of a New Customer Welcome Kit.
- b. FNM will maintain a record of this notification for a minimum period of one (1) year. The CPNI Integrator will maintain all such records.
- c. Individual notice to customers must be provided when soliciting to use, disclose or permit access to customers' CPNI. The form of the notice and opt-in approval shall be determined by the Company. Any solicitation for approval must be proximate to the notification of the customer's CPNI rights.

2. FNM's notification to customers of their CPNI rights will provide sufficient information to enable the customer to make an informed decision as to whether to permit FNM to use, disclose or permit access to the customer's CPNI. The Notice will

clearly state and support the following:

- The customer's right and FNM's duty under federal law to protect the confidentiality of CPNI
- The types of information that constitute CPNI
- Who will have access to CPNI
- How it will be used
- The customer's right to disapprove the uses and to deny or withdraw access to CPNI at any time
- The specific steps the customer must take to grant or refuse access to CPNI
- A denial of approval will not affect the provisioning of any services to which the customer subscribes
- A brief description of consequences resulting from the lack of access to CPNI
- Is clear and comprehensible
- States that lack of approval will prohibit FNM's ability to provide information on other services
- Any customer approval or denial for use of CPNI outside of the service to which the customer already subscribes is valid until they so change it
- The process customers must do to grant or deny approval
- No attempt to encourage a customer to freeze-third party access to CPNI The Vice President of Finance shall be responsible for reviewing and approving the form and content of the Notice to customers. The Company may also have the form and content of the Notice reviewed by its legal counsel. The CPNI Integrator shall be responsible to ensure that the Notice is timely mailed to the then-existing customers of FNM's telecommunications services.

3. FNM will wait a 35-day maximum period of time after mailing the Notice to customers and an opportunity to opt-out before assuming customer approval to use, disclose or permit access to CPNI. FNM's Notice will advise customers they have 35 days from the date of the mailing of the Notice or their installation to inform the Company of their decision to prohibit the use of CPNI. In the case of individual notice to a customer seeking affirmative written approval as described in Section IV(1), the 35-day waiting period is inapplicable.

4. The Company will not use an electronic method (i.e., e-mail) to provide notification or to obtain customer approval.

5. Customers will have the option at no additional cost to contact FNM at any time to change their CPNI approval status. FNM can be reached electronically, verbally or in writing 24 hours a day, seven days a week. Emails will be sent to subscriber. privacy@FNMI.com. The CPNI Integrator will monitor all emails. Telephone access will be routed to Customer Service. All written correspondence regarding CPNI will be routed to the CPNI Integrator. Any FNM personnel receiving the customer notification will promptly provide Customer Service with the following information: date and time of call, customer name and address, CPNI approval or denial.

6. FNM may use oral notice to obtain one-time consent for the use of CPNI for inbound and outbound customer telephone contacts limited to the duration of the call, regardless of whether the Company uses opt-out or opt-in approval based on the nature of the contact. The contents of any such customer notification must comply with the requirements of paragraph 2 above, except that the FNM representative may omit any of the following notice provisions if not relevant to the limited use for which the Company seeks CPNI:

- a. The representative need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;
- b. The representative need not advise customers that FNM may share CPNI with any affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in the use by, or disclosure to, an affiliate or third party;
- c. The representative need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as the representative explains to customers that the scope of the approval FNM seeks is limited to one-time use; and
- d. The representative may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the representative clearly communicates that the customer can deny access to the CPNI for the call.

VI. SAFEGUARDS REQUIRED FOR USE AND RELEASE OF CPNI

1. FNM has implemented a system by which the status of a customer's CPNI approval can be clearly identified and established prior to the use of CPNI. FNM will utilize its billing system to track a customer's CPNI consent status. An alert comment labeled "CPNI-PENDING 35 DAY APPROVAL – DO NOT SOLICIT" will be automatically populated on any new customer's account during the initial service order entry. Once the 35 days has lapsed, the system will automatically remove the comment. The customer's account record will then be coded to reflect the status of approval for marketing solicitation purposes. Located

on the customer's CPNI service screen is an area labeled "RESTRICT SHARING", which when checked indicated the customer has denied use of their information for solicitation of other non-related services. "UNCHECKED" will mean approval has been granted and will be automatically populated as part of the initial service order.

2. At the time a customer denies or withdraws approval, a service order will be completed by Customer Service, which will attach the following alert comment: "NOT AUTHORIZED – DO NOT SOLICIT." At the same time, the CPNI service screen will be updated and the "RESTRICT SHARING" box will be checked at which time the words "RESTRICT AFFILIATE" will appear in red in the upper right on each screen viewed within the customer's account. The system will automatically note the date of the change and approval. As part of the CPNI service screen, the Customer Service representative will choose from a drop down menu whether notice from the customer was received in the following manner: "W" is for written notice; "O" is for oral notice (for all oral notices Customer Service will add a comment to the customer's account noting the date and time of the call and by whom); "E" is for e-mail notification. Both the alert comment and CPNI information screen provides dual opportunities to view a customer's approval status by authorized FNM personnel.

3. New customers will receive a Protecting Your Privacy notification in each Welcome Kit. The Broadband Service Center department will be responsible for dating the notification, as well as inserting into the Welcome Kit. At the time of installation, the technician confirms a customer's receipt of the notice by checking the CPNI box on the service order. The Broadband Service Center will be responsible for inspecting each returned service order for any unchecked CPNI box. Unchecked orders will be given to Customer Service to mail a second notification to the customer and modify the 35-day alert comment date. It will be the responsibility of Customer Service and Finance Department to monitor, maintain and update the customer records.

4. All authorized FNM employees must check the system to verify a customer's approval before using, disclosing or permitting access to a customer's CPNI.

5. FNM implemented additional CPNI safeguards consistent with the FCC's rules by December 8, 2007 by requiring a customer to supply a password before the release of call detail records can be made. FNM will use its billing system to track and administer customer passwords allowing appropriate FNM personnel immediate access for verification purposes. At the time of initial sign-up service, the customer is given the option to choose a non-biographical or non-account related password. If no choice has been made, the system generates a password automatically at the time of the initial service order. The password parameters are alpha-numeric, with a minimum of six (6) characters long and containing at a minimum four (4) numeric digits and two (2) alpha characters. An answer to a pre-determined back-up authentication question is asked during the initial sign-up process. After a customer's services have been installed, a copy of either their selected or system generated password is mailed to the address of record. If the customer has not chosen an answer to the back-up authentication question, a form is also mailed along with their password requesting the customer to provide an answer and return with their first payment. Existing customers were assigned a system generated password, which was mailed to the address of record along with a form requesting an answer to the pre-determined back-up authentication question. Changes in a customer authentication password, address of record, back-up authentication answer or e-mail address could occur when the following situations arise; customer decides to make changes; typographical error was made during order entry; or billing system file loses data. Such notification is not required when the customer initiates service, including selection of a password.

FNM personnel will notify the customer using the following steps:

1. Customer verification is required prior to any changes be made to the account.
2. Once approved the record change must be entered into the billing system.
3. Immediate customer notification can occur in the following manner:
 - Customer is notified by calling the telephone of record and leaving a voice message.
 - System changes are tracked, which produces a file for the purpose of generating a CPNI Authentication Change letter, which is mailed immediately to the address of record.
 - Electronic message can be used as a means of notification provided a customer is using FNM e-mail service.
 - Billing system files are backed up daily, so in the event data is lost, the data can be restored.

The Company will require customers requesting CPNI information or account changes during a visit to a retail location, to either have their password or valid photo identification. FNM will not mail CPNI information to a customer's address of record until it has been associated with the account for a minimum of thirty (30) days. FNM has made significant progress towards compliance with FCC requirements for on-line customer access to CPNI and anticipates completion by the FCC's June 8, 2008 implementation deadline. Under current procedures, a customer using the on-line account review or electronic bill pay is first prompted to enter their pre-assigned password. If the customer should forget or enter incorrectly, a link labeled "FORGOT YOUR PASSWORD" is available. The customer enters their account number, which populates the back-up authentication question. After four (4) unsuccessful attempts are made to log-in, an alert message appears prompting the customer to contact the Customer Service Department.

Once the customer has logged in successfully the option will be available to change the pre-assigned password, answer to the back-up authentication question or electronic address. When information is changed on-line the billing system tracks CPNI Authentication changes for the purpose of generating a CPNI Authentication Change notification letter, which will be mailed to the address of record noting a change was made to the customer's account.

Customer authentication is not required provided the customer can without assistance from an FNM Customer Service representative provide all the of the call detail information necessary (i.e., the telephone number, when it was called and if applicable the amount charged for the call) to address a customer service issue.

To ensure added CPNI security, business customers who reach our Customer Service Representatives will be required to adhere to the same password or back-up authentication procedure when requesting call detail record information or on-line account access.

6. FNM personnel will be trained on the proper authorized use of CPNI and the restrictions on releasing call detail record information without proper authentication and this Policy and Procedure. New employees will receive individual CPNI training as part of their normal orientation. In addition, all Company employees will receive annual training. The annual training will consist of a meeting with all Company personnel during January-February of each year to review and discuss the CPNI Policy and Procedure, including updates or changes in legal requirements or business practices. The CPNI Integrator and Human Resources will conduct the training. The training will consist of reviewing the Company's CPNI policies and examples of acceptable and non-acceptable practices. A question and answer session will follow the training session.

7. Any individual who is found to have used CPNI in violation of this Policy and Procedure will be subject to disciplinary action up to immediate dismissal as outlined in the Company handbook.

8. FNM will maintain a record for one (1) year of its sales and marketing campaigns that use its customer's CPNI information. An electronic file will be kept noting the date, description of the campaign, products and services promoted, delivery method, how many distributed, outside firm used and the specific CPNI used. The Wholesale Markets & Video Content Manager will serve as a member of the FNM Marketing team and will be responsible for maintaining this file.

9. The Vice President of Finance or designee shall also maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. Any FNM personnel discussing the disclosure of CPNI to a third party shall promptly report the incident to the Vice President of Finance.

10. FNM will maintain a supervisory review process regarding its compliance with the FCC's CPNI rules for outbound marketing situations. FNM Sales personnel will be instructed in the proper CPNI authorization needed prior to any outbound sales efforts. This will include obtaining supervisory permission from the Wholesale Markets & Video Content Manager of any proposed outbound marketing request for a customer's CPNI approval.

11. FNM's Chief Financial Officer will be responsible to verify all CPNI policies and procedures are being adhered to by Company personnel. Included will be an inspection of any disciplinary actions that occurred during the prior year. Once this has been completed, the Chief Financial Officer will prepare a written statement to such verification, as required by FCC regulations and will file its certification and compliance statements with the Commission on or before March 1 annually.

12. FNM will provide written notification within five (5) business days to the FCC describing any Instances where the opt-out mechanism did not work properly. The notification will be in the form of a letter and will include the following: Company name, a description of opt-out mechanism used, the problem(s) experienced, the proposed remedy and implementation date, whether the Minnesota Public Utilities Commission has been notified and whether it has taken any action, a copy of the notice provided to customers and contact information.

13. FNM has taken additional reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI information. FNM personnel have been properly trained on how to properly authenticate a customer prior to disclosing CPNI, whether that is a customer initiated telephone contact, on-line account access or an in-store visit. FNM follows industry-standard practices to take such actions as are necessary to prevent unauthorized access to personally identifiable information by a person other than the subscriber or us. FNM uses a variety of security technologies and procedures to help protect personal information in our customer database. All personal information stored in the FNM database is protected by our controlled facility and by limiting access by using a dual layer of passwords that must be changed on a regular basis. Any information provided over the Internet is protected through the use of encryption, such as the Secure Socket Layer (SSL) protocol. We have implemented strict internal guidelines to ensure that customer privacy is safeguarded at every level of our organization. In the event of a network security breach FNM Network operations personnel will notify the Vice President of Technology immediately. The Vice President of Technology will alert senior management of the severity and the remedies for the attempted

unauthorized access.

14. FNM Vice President of Technology or his designee will within seven (7) days after a reasonable determination that a breach in customer's CPNI has occurred inform via electronic notification to the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) the severity and type of CPNI information that was accessed. Customer or public notification will not occur until the seven (7) days have elapsed or FNM is directed by either the FBI or USSS to delay notification for up to thirty (30) days. FNM Senior Management will at its discretion choose the language and method by which to describe the circumstances to its customers or public. FNM will maintain an electronic record for a two (2) year period of any breaches that have occurred. The record will be maintained by the CPNI Integrator. The record must include when possible the dates of discovery and notification to the USSS and FBI, plus a detailed description of the CPNI that was compromised and the method by which the breach took place.