

8049109

Received & Inspected

FEB 28 2008

FCC Mail Room



DOCKET FILE COPY ORIGINAL

**2007 CPNI
Compliance Manual**

**Matanuska Telephone
Association, Inc.**

TABLE OF CONTENTS

<i>Certificate of Compliance</i>	<i>Page 3</i>
<i>Statement of Compliance</i>	<i>Page 4</i>
<i>Attachment 1</i>	<i>Page 9</i>
<i>Attachment 2</i>	<i>Page 13</i>
<i>Attachment 3</i>	<i>Page 17</i>
<i>Attachment 4</i>	<i>Page 20</i>
<i>Attachment 5</i>	<i>Page 21</i>
<i>Attachment 6</i>	<i>Page 22</i>
<i>Attachment 7</i>	<i>Page 23</i>
<i>Attachment 8</i>	<i>Page 24</i>
<i>Attachment 9</i>	<i>Page 33</i>
<i>Attachment 10</i>	<i>Page 34</i>
<i>CPNI Regulations</i>	<i>Page 35</i>



**Certificate of Compliance
Customer Proprietary Network Information (CPNI)**

Part 64.2009(e) of the CPNI Regulations requires annual certification by a corporate officer that a company is in compliance with Part 64 CPNI rules. The FCC has clarified that it now requires all telecommunication companies to submit their certification to the FCC annually on or before March 1st.

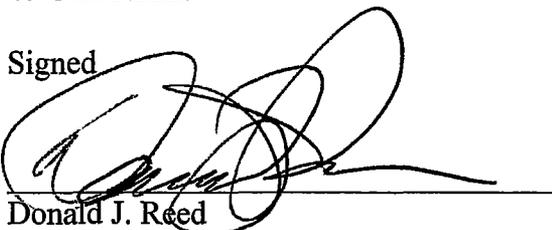
In addition, this record must be kept on file at Matanuska Telephone Association, Inc., to certify the utility's employees have not provided customer proprietary network information or customer information that is protected under 47 U.S.C. 222 to an unauthorized party.

The term Customer Proprietary Network Information means-

- (a) information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service 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
- (b) information contained in the bills pertaining to telephone exchange service or toll service or telephone toll service received by a customer of a carrier.

This letter is certification that I, Donald J. Reed, a company officer attest that I have personal knowledge that the company has established operating procedures to ensure Matanuska Telephone Association, Inc. and its affiliate MTA Communications, Inc. is in compliance with current CPNI regulations. Further, I can attest that for the time period beginning January 1, 2007 and ending December 31, 2007, that no employee of either company has provided customer proprietary network information that is protected under 47 U.S.C.222.

Signed



Donald J. Reed
Director, Regulatory Affairs and Carrier Relations

Dated 2/26/2008

Matanuska Telephone Association Inc.
1740 South Chugach Street
Palmer, Alaska 99645

907.745.3211
800.478.3211 (in Alaska)

www.mtasolutions.com

Local
Long Distance
Wireless
Business Solutions
Internet
Directory
DTV



Statement Accompanying CPNI Certification

Customer Proprietary Network Information

CPNI is defined by the Telecommunications Act as the information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service 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 customer-carrier relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier. CPNI does not include subscriber list information.

MTA Customer Privacy

Matanuska Telephone Association, the local exchange carrier and its affiliate MTA Communications respect and protect member/subscribers' privacy and comply with the Telecommunications Act and associated FCC regulations governing the use of customer proprietary network information (CPNI). Customer service personnel are trained at the outset to keep all customer records confidential. The MTA Customer Service department is committed to the compliance of CPNI requirements. To ensure that all Sales and Customer Service personnel are following CPNI requirements, two written Standard Operating Procedures (SOP) have been implemented: Customer Proprietary Network Information (CPNI), SOP – 544, Revision 3; and CPNI – Customer Verification Code SOP – 545, Revision 5, (See Attachments 1 and 2). These procedures are written by the Customer Care Process (CCP) Analyst who works with several departments and supervisors to develop and update these standards. In addition, the CCP Analyst attends staff meetings of all three Sales and Customer Service offices on a regular basis to disseminate and promote the understanding of these procedures. Updates to CPNI procedures are provided at staff meetings.

New employees are oriented on CPNI policy and procedures by attending a training session with their supervisor. Details of SOP – 544 and SOP – 545 are reviewed during the training session. Topics that are covered include: purpose; procedures; setting up/changing a verification code; scripting; customer forgetting verification code; setting up a security question and answer; former MTA customers; and when you do not need a verification code. Common customer scenarios are discussed in this training. Moreover, new representatives are also paired with experienced representatives who work closely with them. One final measure implemented to ensure quality assurance; customers are notified that calls to Sales and Customer Service are electronically recorded. Supervisors listen to these calls randomly to ensure adherence to CPNI standards. Any questions

Matanuska Telephone Association Inc.
1740 South Chugach Street
Palmer, Alaska 99645

907.745.3211
800.478.3211 (in Alaska)

www.mtasolutions.com

Local
Long Distance
Wireless
Business Solutions
Internet
Directory
DTV



regarding information that can be released are referred to the supervisors. The supervisors follow strict policy regarding the release of information.

All employees at MTA read and acknowledge receipt of MTA's Secrecy of Communications policy at the time of hire, (See Attachment 3). The failure of an employee to observe and follow this company policy is subject to discipline, up to and including dismissal. To add an additional layer of security, MTA now requires all employees who have access to CPNI to read and acknowledge receipt of MTA's CPNI policy, (See Attachment 4). MTA work rules expressly forbid the disclosure of confidential information to anyone unless directed to do so by a supervisor.

MTA further protects the security of its customer's privacy through its electronic network policies. A supervisor's approval is required before an employee has access to any electronic database of MTA's records. Further, MTA takes all reasonable efforts to maintain the security of its electronic network from invasion by unauthorized users.

MTA has implemented the password requirement for CPNI requests into its daily operations. MTA sent out a letter notifying our customers of the change and encouraged them to setup a password and backup authentication method. In the letter it was made clear that the password needed to be non-biographical in nature. MTA gave customers several backup authentication questions and asked them to provide responses. An example of a question used for authentication included asking the customer their favorite color. To ensure a large response, MTA enticed all customers to respond by entering each response into a drawing for a free trip to Hawaii, (See Attachment 5). To further protect customer information which is not considered CPNI, MTA has enacted a company policy that all customers who call in to discuss their account be required to authenticate themselves using the new CPNI authentication methods required by the FCC regardless of whether or not their request falls under CPNI. This approach will ensure that all customer information is protected

The new FCC requirements require CPNI information to only be released after a customer has authenticated themselves. MTA has procedures in place for use when a customer is unable to authenticate themselves by password or backup question. If a customer calls in and forgets their password and is unable to answer a backup question, the customer service representative is required to either call the customer back at their number of record, inform the customer that the information will be mailed to their address of record, or request the customer come in to the office and present photo identification. These alternative authentication methods ensure that customer data remains safe from unauthorized individuals.

If a customer requests to change information on their account or alter their services, a program within the database has been created which automatically flags that person's

Matanuska Telephone Association Inc.

1740 South Chugach Street
Palmer, Alaska 99645

907.745.3211
800.478.3211 (in Alaska)

www.mtasolutions.com

Local
Long Distance
Wireless
Business Solutions
Internet
Directory
DTV



information and a label is generated which is then attached to a mailer and sent out to the customer address of record prior to any changes, (See Attachment 6). The mailer informs the customer a change has been made to their account and a phone number is provided for them if they have any questions.

New customers to MTA are informed about CPNI and why they need to protect their information. Customers are now asked to provide a CPNI password and backup authentication answers at the time the customer initiates service with the company. After the customer has been with MTA for 30 days, a mailer is sent out detailing our CPNI policy and how CPNI is used internally. After 60 days of being a MTA customer, a second letter is sent out informing the customer of our opt-out policy. The mailer informs the customer they have the right to request their information not be used for marketing purposes.

MTA has instituted a breach notification policy which covers both an internet breach and a traditional breach. Both are taken very seriously and handled expeditiously. All customer service reps have been trained to understand the breach policy and what steps need to be followed to report that breach. For a traditional breach, the representative is required to fill out a CPNI Breach Notification Form, (See Attachment 7). This form contains the customer's information, the representative's information who handles the complaint, and finally a narrative of the complaint being reported. This form is then submitted to both the representative's immediate supervisor as well as the Regulatory Affairs Department. All complaints must be submitted within 48 hours of notification internally. Regulatory Affairs then utilizes this information to report the breach via the breach reporting portal, which is required by the FCC. The web address is (<https://www.cpnireporting.gov/dtrp/content/disclaimer.faces>).

As required by the FCC, these complaints are processed within 7 days of the initial complaint. MTA will not notify the customer of the resolution to their complaint until law enforcement has investigated the breach and given permission to proceed with notification.

A internet breach of the customer database or a customer's online portal is handled by our IT department. Their response to the breach is immediate, (See Attachment 8). An incident commander for the breach is assigned, this person is the main contact person for details pertaining to the breach. A severity level will be assigned with 1 being a major incident and 3 being a minor incident. During the processing of the breach, hourly reports are given to the IT managers, as well as the Executive Manager of the IT department. Once the breach has been contained, a formal report is then prepared and sent to Management and Regulatory Affairs for processing. An online breach is handled in a similar fashion as the traditional breach in that the breach is submitted to law enforcement via the breach portal within 7 days of the incident.

Matanuska Telephone Association Inc.

1740 South Chugach Street
Palmer, Alaska 99645

907.745.3211
800.478.3211 (in Alaska)

www.mtasolutions.com

Local
Long Distance
Wireless
Business Solutions
Internet
Directory
DTV



Marketing Campaigns

MTA has implemented the opt-out policy available under the CPNI regulations at CFR 47 §222 (c)(3) for identifying customers who do not wish to have their CPNI used in marketing campaigns. Customers are given the opportunity annually to opt-out of any marketing campaigns that take place during the year. Each customer receives two notices annually. The first notice sent out to customers is a flyer which educates them on CPNI and its possible uses, (See Attachment 9). The second notice sent out 30 days later is a letter which informs the customer that MTA has adopted an opt-out policy. The customer is asked to do nothing if they want to be part of marketing campaigns. If the customer chooses to opt-out, they are given several options for contacting MTA. We give them the option of calling us, emailing us, or the traditional method, by regular mail. Customers are asked to respond within 30 days if they choose to opt-out, (See Attachment 10). If at anytime a customer who has not opted out changes their mind, they can choose to opt-out at any time during the year by using the same methods discussed above.

To ensure proper accounting of CPNI status for a customer is accurate, all customer data maintained in the database is assigned a specific indicator as to their CPNI status. All customers who notified us that they are opting out are assigned a flag within the system alerting Marketing and Customer Service that this customer wishes to be excluded from any marketing campaigns. Those customers who have not chosen to opt-out have a comment in the CPNI field indicating that the customer's CPNI may be utilized in connection with advertising campaigns. The CPNI field within the database can only be changed by the creation of a service order. When a marketing campaign is being planned, a query is run on the customer database and all customers who have the opt-out flag assigned to them are purged from the list. The final customer list contains only those customers who have not opted-out. All marketing campaigns are tracked by a database which contains the campaign name, date it was initiated, and how CPNI information was used for that specific campaign. The database is maintained by the Marketing department and is purged annually.

Complaints and Filings Regarding CPNI

During the calendar year beginning January 1, 2007 and ending December 31, 2007, MTA and its affiliate MTA Communications received zero complaints in regards to CPNI usage or breaches. During this same calendar year no reports or proceedings were initiated by Matanuska Telephone Association, Inc. or it's affiliate MTA Communications, Inc. against data brokers to the FCC or the Regulatory Commission of Alaska. MTA is aware that pretexters and their ability to obtain data are a major threat to customers and MTA has instituted all requirements by the FCC into the daily operations

Matanuska Telephone Association Inc.

1740 South Chugach Street
Palmer, Alaska 99645

907.745.3211
800.478.3211 (in Alaska)

www.mtasolutions.com

Local
Long Distance
Wireless
Business Solutions
Internet
Directory
MTA



of the company as well as implementing procedures for protecting non-customer detail information. By instituting the procedures explained in this statement, MTA believes it is doing everything in its power to protect our customer's CPNI information.

Matanuska Telephone Association Inc.
1740 South Chugach Street
Palmer, Alaska 99645

907.745.3211
800.478.3211 (In Alaska)

www.mtasolutions.com

Local
Long Distance
Wireless
Business Solutions
Internet
Directory
DTV

MATANUSKA TELEPHONE ASSOCIATION



Status: Final

Standard Operating Procedure

TITLE: Customer Proprietary Network Information (CPNI)

NUMBER: SOP – 544

REVISION: 3

REVISION DATE: January 9, 2008

APPROVALS:

Crystal Nunley,
Customer Care Process Analyst

Date

Joe Slagle, Regulatory Affairs Analyst

Date

1.0 PURPOSE

CPNI is customer data that is not publicly available and includes information such as type of service, number of telephone lines, amount of usage, calling records and billing records. Customers have the right to authorize telephone companies to share this information with subsidiaries and external companies or to keep this information confidential.

2.0 REFERENCES

SOP 609 – Additional Contact Information

3.0 DEFINITIONS

CPNI - Customer Proprietary Network Information

4.0 PROCEDURE

4.1 The CPNI records are maintained at the customer level and contain flags that indicate whether or not the customer gave permission for their information to be shared internally or externally.

4.1.1 These records are created when a customer is created during the Service Order process.

4.1.2 Once a customer has been created the CPNI information can be edited within Service Order, Inquiry or GUI.

MATANUSKA TELEPHONE ASSOCIATION



Status: Final

Customer		5/25/07	9:16:49
Customer#	120931		
First Name	DIANA		
M.I.	L		
Last Name	ESCOBAR		
Title			
SSN/Tax ID			
Reach At Phone Number			
Gender	F	Race	U
Customer Proprietary Network Information (CPNI):			
Internal Flag	I	External Flag	I
CPNI Comment	_____		
F3=Exit F4=Prompt F13=Fast Exit F14=Credit History F15=CPNI History			

- 4.1.3 The default for the internal and the External Flag is always I for Opt In.
- 4.1.4 MTA has chosen not to use the External Flag field since we do not share our customer's information with outside companies.

4.2 Sending Opt-Out Request notification

- 4.2.1 The initial CPNI notifications will be sent in the June 15 and July 1, 2007 statements. After the notification are sent MTA must wait 30 days before assuming customer approval to use, disclose, or permit access to their CPNI.
- 4.2.2 Subsequent notices will be sent out on an annual basis every June.
- 4.2.3 Each time a new customer number is created in CommSoft this customer will receive the notice.

4.3 No Response from Customer

- 4.3.1 If there is no response from the customer there is no action necessary within CommSoft.
 - 4.3.1.1 Essentially, by not responding the customers are saying they don't mind if we use their CPNI information for marketing purposes.

4.4 Customer Opts Out

- 4.4.1 The customer has a couple of ways to opt out by phone or by email. The email will be sent to mtaprivacy@mta-telco.com. The emails will be included in the customer care emails.
 - 4.4.1.1 From Inquiry, select Option 30 to update.
 - 4.4.1.2 From within a service order, go to Customer screen and (2) to edit.
 - 4.4.1.3 Change the Internal Flag from I to O for Opting Out (This field is also promptable.)
 - 4.4.1.4 Enter to confirm the change
- 4.4.2 Update both the Responsible and Co-Responsible Parties.
 - 4.4.2.1 Do not flag any other roles such as Adult with Access or Billing Contacts.
- 4.4.3 If the request to opt out comes in through an email please record the email address if it is not an MTA Online address on the Service Account Contacts Screen (See SOP 609).

MATANUSKA TELEPHONE ASSOCIATION



Status: Final

4.5 Returned Mail

4.5.1 MTA will make a second attempt to get the CPNI notice to the customer; however, if the notice comes back a second time, then:

4.5.1.1 We will change the flag and show the customer as Opted out.

Customer Proprietary Network Information (CPNI):
Internal Flag 0 External Flag 1
CPNI Comment _____

4.5.1.2 We will place comments on the account.



4.6 CPNI Audit History

4.6.1 Once the change has been confirmed an Audit trail is created tracking the History of when the customer opted in or out.

4.6.1.1 This information can be viewed in customer inquiry by selecting option 30, then pressing F15.

Customer			CPNI Audit History			5/25/07 9:31:21	
Internal Flag	External Flag	Comment	Action Last User	Action Last Date	Action Last Time		
I	I		CONVERSION	11/20/05	1:55:16		

5.0 RECORDS

- CPNI Audit History

6.0 CHANGE CONTROL

6.1 Document Revision History

Date Changed	Revision #	By Whom	Changes(s) Made	Date Emailed to Business Partners
5/24/07	0	Diana Escobar	Created	NA
6/6/07	1	Diana Escobar	Changes from Validation	Wk of 6/11/07 Staff Meetings
8/3/07	2	Diana Escobar	Added returned mail info	8/6/07 SalesMark
01/09/08	3	Crystal Nunley	Updated 4.5	Staff Meetings starting 01/10/08

6.2 Notification of Changes

Include Statement to the Business Partners of substantive changes made to this document:

Business Partner Name	Role / Title	Email Address
Marketing		marketing@mta-telco.com
Joe Slagle	Regulatory Affairs	jslagle@mta-telco.com

MATANUSKA TELEPHONE ASSOCIATION



Status: Final

Residential & Wireless Customer Service		<u>Cs-everyone@mta-telco.com</u>
Business Customer Service		<u>Bsc1@mta-telco.com</u>
Repair & Dispatch		<u>Repair_dispatch@mta-telco.com</u>
Billing		<u>NetBill_Admin@mta-telco.com</u>

MATANUSKA TELEPHONE ASSOCIATION



Status: Final

Standard Operating Procedure

TITLE: CPNI – Customer Verification Code

NUMBER: SOP – 545

REVISION: 5

REVISION DATE: January 15, 2008

APPROVALS:

Crystal Nunley,
Customer Care Process Analyst

Date

Joe Slagle, Regulatory Affairs Analyst

Date

1.0 PURPOSE

Starting 12/08/07, new FCC regulations require that we collect a password from our customers to identify them prior to giving out or changing account information. MTA will call this password a **customer verification code** so that we can differentiate it from the other passwords we have for our customers.

In most situations we have been verifying the last 4 digits of the customers SSN. These new regulations no longer allow us to ask the customer their SSN, account information or biographical information in order to identify them. The customer needs to set their own verification code.

MTA will continue to collect the customers SSN for credit and collection purposes.

2.0 REFERENCES

- FCC 07-022
- SOP – 544

3.0 DEFINITIONS

- PIC – Primary Inter-exchange Carrier

4.0 PROCEDURE

4.1 **General Information**

- 4.1.1 All Customer Care Associate's need to ask for a customer's verification code at the beginning of every conversation.
- 4.1.2 All Customer Care Associate's need to view whether the customer has Opted Out for Marketing purposes. See SOP – 544.
- 4.1.3 **NO PROMPTING IS ALLOWED**
Examples:
 - 4.1.3.1 What is your SSN?
 - 4.1.3.2 What is your date of birth?
 - 4.1.3.3 What is your Alaska drivers license number
- 4.1.4 If you need further CPNI clarification, then please see your supervisor.

4.2 **Setting up/Changing a verification code**

- 4.2.1 If a customer does not have a verification code, then you can ask a customer, "What was the password you provided us in the past?"

MATANUSKA TELEPHONE ASSOCIATION



Status: Final

- 4.2.1.1 If the customer answers with their SSN, ADL or DOB (without prompting) and it is correct, then you can set up a customer verification code.
 - 4.2.2 When setting up a verification code, explain to the customers;
 - 4.2.2.1 "Please choose a verification code that is easy for you to remember."
 - 4.2.2.2 "You will need to provide this verification code in the future for any changes or inquiries on your MTA account."
 - 4.2.3 All parties on an account (responsible, co-responsible, adult with access, etc.) can have separate verification codes.
 - 4.2.4 The verification code needs to fit into the following parameters:
 - 4.2.4.1 3 to 10 alpha numeric characters
 - 4.2.4.2 No spaces or symbols
 - 4.2.4.3 Not case sensitive
 - 4.2.5 A new service order type has been created to make changing the verification code easier. This service order type is a: TPW.
 - 4.2.5.1 This service order type will only go to the customer screen where you enter the verification code into the password field.
 - 4.2.6 Once the verification code is set up, then the rep will write the verification code on a blank MTA business card to give to the customer.
- 4.3 **Customer Forgot Verification Code**
- 4.3.1 They have only four options (as set out by the FCC) we can use to give them the verification code they have forgotten:
 - 4.3.1.1 Come into the office and show ID. At that time, the rep can then give them their verification code.
 - 4.3.1.2 Rep can mail the verification code but only to the address on the billing statement.
 - 4.3.1.3 Rep can call the customer back at a phone number that in on the billing statement. At that time, the rep can then give them their verification code.
 - 4.3.1.4 Customer can provide answer to the security question that they set up. At that time, the rep can then give them their verification code.
- 4.4 **Setting up a Security Question and Answer**
- 4.4.1 Properly identifying a customer (4.3.1.1, 4.3.1.2 or 4.3.1.3).
 - 4.4.2 Determine the security question and answer the customer would like to use. You may use one of the following 5 question/answers:

Question to ask Customer	Question/Answer typed in CommSoft (examples)
What is your favorite color?	Favorite color = Purple
What is the name of your favorite pet?	Favorite pet = Spot
What is your shoe size?	Shoe size = 7
What is your favorite vacation spot?	Favorite vacation = Hawaii
What is your favorite sibling's middle name?	Sibling's middle name = Alan

- 4.4.3 Bring up the customer's account
 - 4.4.3.1 Enter option 30 (Customer Number)
 - 4.4.3.2 Enter the question/answer that the customer would like to use on the CPNI comment line

MATANUSKA TELEPHONE ASSOCIATION



Status: Final

4.6.2.1 They are then allowed to make other CPNI protections than those required by the FCC.

4.7 When a former MTA customer is calling about their disconnected account, then the same CPNI procedures apply.

4.8 When you do not need a verification code

4.8.1 There is ONLY one situation that a rep CANNOT ask for a verification code from a customer. This is when a customer is calling to change their PIC.

4.8.2 When a customer is ONLY paying a bill.

5.0 RECORDS

- Service Order
- Audit History

6.0 CHANGE CONTROL

6.1 Document Revision History

Date Changed	Revision #	By Whom	Changes(s) Made	Date Emailed to Business Partners
8/22/07	0,1,2	Diana Escobar	Created	Wk of 8/27/07 staff meetings
9/21/07	3	Diana Escobar	Password changed to verification Code	Email 9/21/07
12/07/07	4	Crystal Nunley	Update Procedure with security question & answer	Wk of 12/18/07 staff meetings
01/08/08	5	Crystal Nunley	Revised Purpose, 4.1, 4.2, 4.3, 4.6, 4.7, 4.8	

6.2 Notification of Changes

Include Statement to the Business Partners of substantive changes made to this document:

Business Partner Name	Role / Title	Email Address
Billing		NetBill_Admin@mta-telco.com
Marketing		marketing@mta-telco.com
Residential & Wireless Customer Service		Cs-everyone@mta-telco.com
Business Customer Service		Bsc1@mta-telco.com
Joe Slagle	Regulatory Affairs Analyst	jslagle@mta-telco.com
Dispatch/Repair		Repair_dispatch@mta-telco.com

MATANUSKA TELEPHONE ASSOCIATION, INC. WORK RULES

The following is a list of general work rules. These rules are not meant to hinder or restrict you, but rather to insure safer working conditions and create a more pleasant environment. These basic rules are being distributed in this handbook so that you know what is expected of you and the progressive discipline process.

It is assumed that most employees, once aware of the work rules, will voluntarily comply with them. For those few individuals who do violate work rules, MTA subscribes to the philosophy of progressive discipline.

Progressive discipline is designed to correct inappropriate behavior. Ordinarily, you will be given verbal counseling, a written warning, suspension and finally discharge, if the behavior persists.

However, for violations involving violence, intimidation, insubordination, harassment, unauthorized removal of property or other acts of gross misconduct, some or all of the normal progressive discipline steps may be waived at the discretion of your supervisor and in conjunction with the Human Resource Manager. Because of the relatively short work period for seasonal employees, they can generally expect discipline to be levied at a more accelerated rate than for the regular employees. (For further information, refer to the MTA Progressive Discipline SPP.)

It is your responsibility as an MTA employee to understand and conform to all work rules. Additionally, you are responsible for maintaining all requirements of your job (e.g. driver's license). If you have any questions concerning a work rule or the related disciplinary action, discuss it with your supervisor so you will have a complete understanding of each item.

It is your supervisor's responsibility to enforce these rules equitably and uniformly. In accordance with the Progressive Discipline Policy, enforcement shall be accomplished with a full understanding of all the facts and circumstances surrounding any violation.

In each case the severity of the penalty shall be appropriate to the offense. The supervisor shall consider all mitigating and extenuating circumstances.

1. Producing or permitting a false record relating to time worked or materials used is prohibited.
2. Discrimination on the basis of race, color, religion, sex, age, disability or national origin will result in disciplinary action, up to and including discharge. (Refer to the Notice of Non-discrimination.)
3. Under no circumstances will sexual harassment be tolerated. Such harassment includes unwelcomed sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature.
4. You shall not disclose confidential information to anyone unless directed to do so by your supervisor.

**MTA NOTICE
OF
SECRECY OF COMMUNICATIONS**

1. Employees must not disclose the contents, or any part of **ANY** message addressed to another person without the permission of the sender, or willfully alter the purport or effect of meaning of any such message. (This includes but is not limited to telephone, radio, fax, and telegraph messages). Both parties to a telephone conversation are considered senders.
2. Employees must not use any information, derived from any private message passing through their hands and addressed to another person, or in any other manner acquired as an employee of the company.
3. Employees must not permit any unauthorized person to listen to any telephone conversation. Employees must not monitor any connection more than is needed for its proper supervision.
4. Employees must not discuss communication arrangements made between the company and its customers, except as required for handling business properly.
5. Employees must not discuss the fact or the nature of any message with anyone, except as required for handling it properly.
6. Employees must not give any unauthorized person any information whatsoever about the location of equipment, trunks, circuits, cables, etc., or information concerning local or toll ticket records or class, teletypewriter or fax messages, etc.

The secrecy of communications is protected by law imposing punishment by fine (up to \$10,000) and imprisonment (up to 2 years) for its violation.

**MTA
EMPLOYEE ACKNOWLEDGMENT AND SIGNATURE FORM**

By signing this form I, certify and acknowledge that I have received a copy of each of the listed documents and polices and that I have read and understood them.

- 1) EEO Document Letter
- 2) MTA Statement of Non-Discrimination
- 3) MTA Non-Discrimination in Provision of Service Policy (Title VI)
- 4) MTA Non-Discrimination in Employment Policy (Title VII)
- 5) Sexual Harassment Policy Statement and Alaska Commission for Human Rights "Sexual Harassment Information Notice"
- 6) Your Rights Under the Family and Medical Leave Act of 1993
- 7) Notice of Secrecy of Communications
- 8) Notification of Requirement to Maintain Valid Driver's License
- 9) Notice on Search and Inspection of MTA Owned and Operated Property
- 10) Electronic Information & Communication Systems Employee Notification
- 11) Internet Acceptable Use Policy
- 12) Assignment of Inventions

I further understand and acknowledge that the failure of any employee to observe and implement such policy constitutes grounds for disciplinary action up to and including dismissal.

Employee Printed Name: _____

Employee Signature: _____

Date Signed: ____/____/____

Supervisor's Signature: _____



Customer Proprietary Network Information, (CPNI) is information pertaining to call detail. Call detail includes phone numbers called, frequency and duration of calls, as well as specific customer account information which identifies specific services subscribed to by the customer. Employees of MTA have access to sensitive customer information each and every day. It is the duty of each employee to ensure that data is secure and protected from being used in malicious manner. As an employee you must agree to protect this information and stipulate to the following policy:

- I understand that any information concerning a customer's network telephone services should be treated in a confidential and proprietary manner.
- I understand that without customer approval, individual CPNI may only be accessed, used, or disclosed to provision (a) the telecommunications service from which the information is derived or (b) services necessary to, or used in the provision of such telecommunications services.
- I understand that without prior approval of the customer, I may not use individual CPNI to market nonregulated services such as DTV, DSL, or Wireless Telephone.
- I understand that proprietary information that MTA receives or obtains from another telecommunications carrier for purposes of providing telecommunications service may only be used for providing that service and may not be used for MTA's own marketing purposes.
- I will not try to access individual CPNI which I am not authorized to review.
- I will not utilize any individual CPNI which I am not authorized to access.
- I will not disclose individual CPNI to unauthorized personnel or unauthorized parties.
- I will follow all procedures set forth to protect a customer's information from being compromised.

Any deviation from this policy will result in disciplinary action consistent with the official MTA policy in place.

Employee Signature

Date



**Return The Attached Card By October 15
And You Could Win A Trip To Hawaii!**

September 19, 2007

Dear MTA customer:

In recent years, the FCC (Federal Communications Commission) established rules in an effort to protect consumer privacy. To further protect the privacy of telecommunications consumers, the FCC recently passed CFR (Code of Federal Regulations) Title 47 Part 64.2010. This new regulation mandates that all telecommunications companies must allow customers to create a confidential verification code in order to verify their identity when accessing account information.

How are MTA customers affected?

Beginning October 2, 2007, this verification code will be requested by us when you conduct business with MTA. Some types of uses for the verification code include: paying your bill online, adding or removing services to your account, billing questions, and requesting statement copies. This new level of security is intended to provide more privacy and security for you.

It is important for you to act now to establish your personal and confidential verification code. Your code can be 3 – 10 characters in length and contain letters and numbers only. No symbols and no spaces, please.

The FCC provides the following three options for setting up your verification code:

1. Mail your verification code to MTA on the tear-off card attached to this letter. The card will be destroyed after your account has been updated.
2. Establish your code in person at one of our store locations in Eagle River, Palmer or Wasilla.
3. Call MTA at 800-478-3211 or 745-3211, from the main phone number that is listed at the top of your MTA statement. (Important if you have a consolidated statement).

We appreciate your prompt reply, which will allow MTA to serve you in the future with the least amount of inconvenience.

Carolyn Hanson
Director of Marketing

Matanuska Telephone Association Inc.
1740 South Chugach Street
Palmer, Alaska 99645

907.745.3211
800.478.3211 (in Alaska)

www.mtasolutions.com

- Local ■
- Long Distance ■
- Wireless ■
- Business Solutions ■
- Internet ■
- Directory ■
- DTV ■

SET UP YOUR NEW VERIFICATION CODE BEFORE OCTOBER 15, 2007 AND WE'LL ENTER YOU INTO A DRAWING TO WIN A TRIP TO HAWAII. WE'RE GIVING AWAY 15 TICKETS TOTAL. HURRY. (Sorry: MTA employees are not eligible.)

Keep this side with your new verification code
in a safe place.

Mail this side to MTA in the postage-paid
envelope. This is also your entry for a trip
to Hawaii.

Your main phone number
(Found at the top of your MTA statement.)

Your main phone number
(Found at the top of your MTA statement.)

(_____)
MTA customer verification code
3 – 10 characters. Numbers and/or letters only, no spaces
or symbols.

(_____)
MTA customer verification code
3 – 10 characters. Numbers and/or letters only, no spaces
or symbols.

REGARDING YOUR CUSTOMER PRIVACY NOTICE

This notice is to let you know that MTA has recently received your change of address and/or your newly changed MTA verification code.

This notice is required by the (FCC) Federal Communications Commission.

No action is necessary; however, if you have not authorized this change please contact MTA immediately at 800-478-3211 or 694-3211 or 745-3211.

Thank you for your help keeping your records current.



Palmer, Eagle River & Wasilla
745.3211 or 800.478.3211
mtasolutions.com



Matanuska Telephone Association, Inc.

CPNI Customer Service Breach Notification Form

Customer Account Information

Full Name: _____
Last *First* *M.I.*

Address: _____
Street Address *Apartment/Unit #*

_____ *City* *State* *ZIP Code*

Home Phone: () _____ Alternate Contact Phone: () _____

E-mail Address: _____

MTA Member Number: _____

MTA Information

Customer Service Representative Who Handled Initial Complaint: _____ Employee ID: _____

Supervisor: _____ Department: _____

Work Location: _____ E-mail Address: _____

Work Phone: () _____ Date Complaint Received: _____

Complaint Information

Provide a brief narrative of the complaint below:

All Complaints must be submitted to Regulatory Affairs within 48 hours of the complaint being received.

E-Mail to Regulatory Affairs

Print Form



IT Incident Response Process

Listen - Commit - Deliver

Incident Response Process

PROCESS NAME: IT Incident Response

AUTHORITY: IT Director

PURPOSE: MTA relies on numerous information systems and computer files for conducting, facilitating, and monitoring its telecommunications business. The availability and integrity of these systems and their data is critical to the high quality of services provided to MTA's members. The primary objective of MTA's Incident Management is to return the client to service as quickly as possible with a minimum impact to the computing environment.

CONTENTS:

1. Objective
2. Roles and Responsibilities
3. Process Description
4. Approval
5. Revision of Document

Appendix A - IT Incident Response Matrix
Appendix B - IT Major Incident Formal Report
Appendix C - Glossary of Terms

1. OBJECTIVE

This document describes IT's Incident Management Process. The target audience for this document includes groups providing IT support or developing systems for production. It is meant to provide a detailed overview of the Incident Management service definitions, as well as high level descriptions of the process including incident information flow, technology and tools required and operations scenarios. This process will be reviewed at least annually at the direction of the IT Director.

2. ROLES AND RESPONSIBILITIES

2.1 **Process Owner:** IT Manager

2.2 **Roles:** This section provides a brief description of the key responsibilities of individuals who are referenced in the Incident Management Process.

Incident Commander (IC): The Incident Commander is the primary focal point once a major incident occurs or a minor incident has been escalated. This position is to be filled by the IT Manager or his/her designated backup and has the following responsibilities:

- Ensures effective coordination of activities to restore service.
Manages and coordinates all activities necessary to respond to



IT Incident Response Process

Listen - Commit - Deliver

- incidents. Records and resolves incidents by communicating preventative actions and best practices to avoid recurrence.
- Provides a single point of contact for clients looking for information and reporting failures.
 - Coordinates the activities necessary for the immediate short-term resolution of incidents so that clients can resume their work as rapidly as possible following a failure.
 - Ensures that business management is sufficiently informed as to volume, impact and cost of incidents.
 - Primary point of contact for IT to disseminate operational information to the client.
 - Ensures the customer who initially registered the incident formally accepts all solutions.
 - Responsible for retrieving accurate and complete data for the incident analysis.
 - Provides a post incident analysis to determine what can be done to prevent future similar incidents.
 - Audits process to make sure it is being followed. This will be done by quarterly review of formal reports and through the incident management system reporting tools.

Incident Team Lead: The incident team lead is the primary person in charge of the system or application affected. The lead can be called upon by the Incident Commander in the case of a major incident to perform the functions defined below or in the case of a minor incident this person would perform all functions until such time as the incident is closed or escalated. A current list of Systems / Application responsibilities can be found in Appendix A, IT Incident Response Matrix.

- Owns all incidents assigned to them. Communicates and coordinates directly with the Incident Commander / IT Staff.
- Ensures incident is logged and tracked in the Incident Management System.
- Performs activities necessary for the immediate short-term resolution of incidents so that clients can resume their work as rapidly as possible following a service failure.
- Briefs management of status, progress and history of incidents.
- Ensures that the client who initially registered the incident formally accepts all solutions.
- Minimizes the effects of incident on service levels.
- Adheres to authorized procedures and working practices.
- Reduces or eliminates recurring incidents.



IT Incident Response Process

Listen - Commit - Deliver

Incident Response Process

Incident Support Agent: Incident Support Agent is a role that many individuals in IT can perform. Takes direction from Incident Commander or Incident Team Lead as necessary.

3. PROCESS DESCRIPTION

3.1 General Requirements.

1. Every major system / application will have a named primary and backup Incident Support Team Lead. Current coverage is outlined in Appendix A, IT Incident Response Matrix.
2. All trouble calls will be routed through the Help Desk. No exceptions.
3. Every Minor or Major incident will have the following information documented in the Incident Management System (currently TrackIt):
 - Date of event
 - Time of event (if known)
 - Affected systems / applications
 - Description of the problem that will include number of people affected
 - Assigned support agent and initial severity level as described below
 - Document the cause (if known) and solution.

Severity Levels:

Severity 1: Major Incident

Severity 2: Minor Incident requires Incident Team Lead to investigate

Severity 3: Problem that can be solved within normal operations or at time of call

4. Escalation is related to both business impact and urgency, some of which will be a judgment call on the part of IT staff. Generally speaking escalation will occur in the following manner:

Normal troubles will be escalated to Incident Team Lead of affected system or application if any of the following are true:

- Trouble affects 5 to 15 clients.
- Resolution time exceeds 30 minutes.
- Escalated by Incident Team Lead or by Management.



IT Incident Response Process

Listen - Commit - Deliver

Incident Response Process

Minor Incidents will be escalated to the Incident Commander if any of the following are true:

- Trouble affects 15 or more clients.
- Resolution time exceeds 2 hours with no projected resolution time.
- Escalated by Management.

In the event a trouble is escalated the Incident Team Lead or Incident Commander will receive both an email and positive contact notification. In the event the IT staff member doing the escalation does not receive acknowledgment of escalation within 5 minutes the incident will be escalated to the IT Manager or in the case of a Major Incident to the IT Director.

5. In the case of a major incident a formal incident report will be filled out as shown in Appendix B, IT Major Incident Form.
6. After Corrective Action is taken a Failure Analysis will occur. This analysis will provide:
 - Cause of problem.
 - Corrective action taken.
 - Recommendation for any change to production system(s).
7. During the incident, IT management will be updated every hour as to the status of the incident. Either the Incident Commander or Incident Team Lead will keep Business Partners informed as to progress. After the solution is in place, incident will be closed and notification will be sent to clients.
8. For all major incidents, the IT Director will be contacted at the earliest possible convenience by the Incident Commander with status information related to the incident.



IT Incident Response Process

Listen - Commit - Deliver

**Incident Response
Process**

4. APPROVALS

Carl Hereford
IT Manager

Date signed

Dan Monarch
IT Director

Date signed

5. REVISION FOR DOCUMENT

Original Document Creation:	3-31-04
Original Document Revision:	01.00
Original Document Author:	Bev Moore (Process Analyst)

Revision Date	Revision Author	Revision Number	Revision Notes



IT Incident Response Process

Incident Response

Listen - Commit - Deliver

Process

APPENDIX B - IT Major Incident Formal Report

Date and Time of Incident: _____

Incident Commander: _____

Incident Team Lead: _____

Description of Incident (include cause if known):

Impact to the Company:

Actions Taken to Prevent Future Occurrences:

Recommendation for Further Action(s)

Incident Commander Signoff:



Appendix C - Glossary of Terms

TERMS

Applications Systems – Includes application support of financials, service order billing systems, and related databases.

Client – Any MTA employee or department requiring or using IT services or equipment.

Desktop Systems – Includes PC desktop and laptop hardware and operating systems along with any PC Software.

Incident Commander (IC) – Primary focal point for clients and support staff looking for information and reporting failures for major incidents.

Incident Management – The process of restoring service by handling incidents that occur in the infrastructure, including a method for the client to report problems. The purpose of this process is to minimize disruption to the client.

Incident Management System – System used to log and track incident. Currently this system is TrackIt.

Incident Support Agent – Any IT staff person allocated to recording, diagnosing or resolving an incident.

Incident Team Lead – Primary IT staff person on system or applications affected.

Known error – A problem, the cause of which is identified, which requires a long-term solution, regardless of whether a short-term “work-around” solution is available.

Major Incident – An operational event not part of normal operations that cannot be completely isolated and resolved within the limits of a minor incident. Major Incidents typically display one or more of the following characteristics:

- Affects 15 or more clients.
- Increased complexity that goes beyond normal or minor incident resolution times. (minor incident that has been worked on 2 or more hours without a projected resolution time).
- Escalated by management.



IT Incident Response Process

Listen - Commit - Deliver

Incident Response

Process

Midrange Systems – Includes mail system, OS 400s, and "SAN" (Storage Array Network) components.

Minor Incident – An operation event not part of normal operations that cannot be completely isolated and resolved within the limits of normal problem management.

- Affects 5 to 15 clients.
- Increased complexity that goes beyond normal resolution time (time exceeds 30 minutes).
- Escalated by 1st level support or multiple calls on the same issue.
- Escalated by management or Team Lead.

Network Systems – Includes any hardware used to connect WAN or LAN infrastructure.

Production System Change Form (PSCF) – A document that formally requests that a change be performed on an object in production. Objects in production include applications and infrastructure.

Server Systems – Includes server hardware, operating systems, backup, security and remote access.

Support – Is focused on the speedy resolution of incidents. It means: Understanding an event, its scope, and its severity, applying emergency fixes to infrastructure components.

Work-around – An alternative way to perform the function required by the client. Does not fundamentally change the system providing the service and should be considered a short-term solution until a permanent correction can be implemented.

Telecommunications Customer Privacy Rights Notice

What is "Customer Proprietary Network Information" (CPNI)?

CPNI is some of the information MTA obtains in the course of providing telecommunications service to you as a customer. It includes, but is not limited to who, when, and where you call; how much you spend on telecommunications services; which plans you subscribe to; and billing information.

MTA will not sell or provide CPNI to unaffiliated third parties and abides by federal and state CPNI rules that apply to telecommunications carriers. We value our relationship with our customers and are committed to respecting and protecting your privacy. CPNI is used within MTA for billing purposes, to provide and change service, and to contact our customers. With your permission, we may use CPNI to provide you with information on other MTA products and services within the MTA family (for example, Internet, wireless, and digital television) that we think may be of interest to you. These targeted special offers that would help you save time and money may be communicated to you through a variety of ways.

Each year MTA will send out a request for your permission to use your CPNI in order to make you aware of these new and existing products that may best fit your telecommunications needs. You have the right to decline this request. Declining the request will not affect the provision of any services to which you currently subscribe. MTA will honor your decision to decline these offers until you explicitly tell us otherwise.



Palmer, Eagle River & Wasila
745.3211 or 800.475.3211
mtasolutions.com

C

MTA would like to tell you about various ways to receive savings on MTA products and services. But we can't do so unless you allow us to share information internally about your account(s).

How can sharing this information help me?

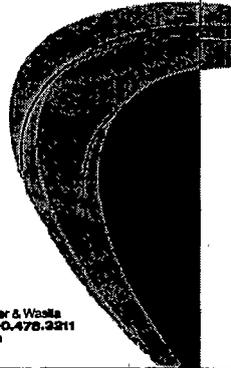
When the MTA customer service representatives see all of the services you currently use, we can make recommendations for new services, new technologies and the most favorable pricing plans that will best meet your communications needs. This could save you money in the long run and, we hope, simplify your life.

Will MTA protect my information?

Definitely. We will never share your information with an outside company. We are only asking permission to share information within MTA. Besides being legally obligated to protect the confidentiality of your information, protecting your privacy is the right thing to do.

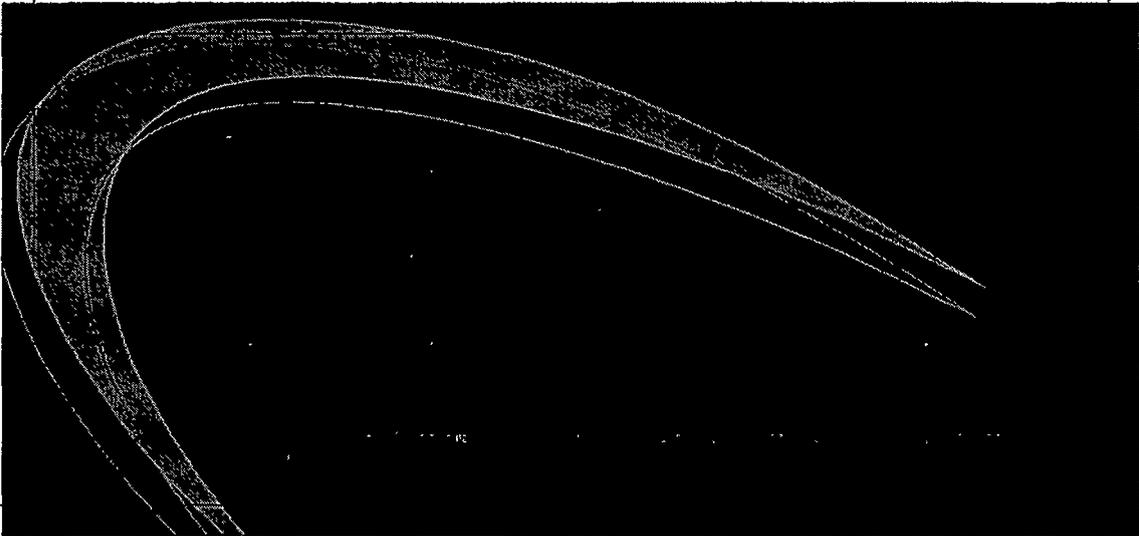


Palmer, Eagle River & Waukegan
748.3211 or 800.478.3211
mitsolutions.com



The MTA logo and the text "Palmer, Eagle River & Waukegan 748.3211 or 800.478.3211 mitsolutions.com" are positioned above a thick black horizontal bar.

C



C

Subpart U—Customer Proprietary Network Information

Source: 63 FR 20338, Apr. 24, 1998, unless otherwise noted.

§ 64.2001 Basis and purpose.

(a) *Basis.* The rules in this subpart are issued pursuant to the Communications Act of 1934, as amended.

(b) *Purpose.* The purpose of the rules in this subpart is to implement section 222 of the Communications Act of 1934, as amended, 47 U.S.C. 222.

§ 64.2003 Definitions.

(a) *Account information.* "Account information" is 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.

(b) *Address of record.* An "address of record," whether postal or electronic, is an address that the carrier has associated with the customer's account for at least 30 days.

(c) *Affiliate.* The term "affiliate" has the same meaning given such term in section 3(1) of the Communications Act of 1934, as amended, 47 U.S.C. 153(1).

(d) *Call detail information.* Any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

(e) *Communications-related services.* The term "communications-related services" means telecommunications services, information services typically provided by telecommunications carriers, and services related to the provision or maintenance of customer premises equipment.

(f) *Customer.* A customer of a telecommunications carrier is a person or entity to which the telecommunications carrier is currently providing service.

(g) *Customer proprietary network information (CPNI).* The term "customer proprietary network information (CPNI)" has the same meaning given to such term in section 222(h)(1) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(1).

(h) *Customer premises equipment (CPE).* The term "customer premises equipment (CPE)" has the same meaning given to such term in section 3(14) of the Communications Act of 1934, as amended, 47 U.S.C. 153(14).

(i) *Information services typically provided by telecommunications carriers.* The phrase "information services typically provided by telecommunications carriers" means only those information services (as defined in section 3(20) of the Communication Act of 1934, as amended, 47 U.S.C. 153(20)) that are typically provided by telecommunications carriers, such as Internet access or voice mail services. Such phrase "information services typically provided by telecommunications carriers," as used in this subpart, shall not include retail consumer services provided using Internet Web sites (such as travel reservation services or mortgage lending services), whether or not such services may otherwise be considered to be information services.

(j) *Local exchange carrier (LEC).* The term "local exchange carrier (LEC)" has the same meaning given to such term in section 3(26) of the Communications Act of 1934, as amended, 47 U.S.C. 153(26).

(k) *Opt-in approval.* The term "opt-in approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. This approval method requires that the carrier obtain from the customer affirmative, express consent allowing the requested CPNI usage, disclosure, or access

after the customer is provided appropriate notification of the carrier's request consistent with the requirements set forth in this subpart.

(l) *Opt-out approval.* The term "opt-out approval" refers to a method for obtaining customer consent to use, disclose, or permit access to the customer's CPNI. Under this approval method, a customer is deemed to have consented to the use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within the waiting period described in §64.2008(d)(1) after the customer is provided appropriate notification of the carrier's request for consent consistent with the rules in this subpart.

(m) *Readily available biographical information.* "Readily available biographical information" is information drawn from the customer's life history and includes such things as the customer's social security number, or the last four digits of that number; mother's maiden name; home address; or date of birth.

(n) *Subscriber list information (SLI).* The term "subscriber list information (SLI)" has the same meaning given to such term in section 222(h)(3) of the Communications Act of 1934, as amended, 47 U.S.C. 222(h)(3).

(o) *Telecommunications carrier or carrier.* The terms "telecommunications carrier" or "carrier" shall have the same meaning as set forth in section 3(44) of the Communications Act of 1934, as amended, 47 U.S.C. 153(44). For the purposes of this subpart, the term "telecommunications carrier" or "carrier" shall include an entity that provides interconnected VoIP service, as that term is defined in section 9.3 of these rules.

(p) *Telecommunications service.* The term "telecommunications service" has the same meaning given to such term in section 3(46) of the Communications Act of 1934, as amended, 47 U.S.C. 153(46).

(q) *Telephone number of record.* The telephone number associated with the underlying service, not the telephone number supplied as a customer's "contact information."

(r) *Valid photo ID.* A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

[72 FR 31961, June 8, 2007]

§ 64.2005 Use of customer proprietary network information without customer approval.

(a) Any telecommunications carrier may use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (*i.e.*, local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

(1) If a telecommunications carrier provides different categories of service, and a customer subscribes to more than one category of service offered by the carrier, the carrier is permitted to share CPNI among the carrier's affiliated entities that provide a service offering to the customer.

(2) If a telecommunications carrier provides different categories of service, but a customer does not subscribe to more than one offering by the carrier, the carrier is not permitted to share CPNI with its affiliates, except as provided in §64.2007(b).

(b) A telecommunications carrier may not use, disclose, or permit access to CPNI to market to a customer service offerings that are within a category of service to which the subscriber does not already subscribe from that carrier, unless that carrier has customer approval to do so, except as described in paragraph (c) of this section.

(1) A wireless provider may use, disclose, or permit access to CPNI derived from its provision of CMRS, without customer approval, for the provision of CPE and information service(s). A wireline carrier may use, disclose or permit access to CPNI derived from its provision of local exchange service or interexchange service, without customer approval, for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

(2) A telecommunications carrier may not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, a local exchange carrier may not use local service CPNI to track all customers that call local service competitors.

(c) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, as described in this paragraph (c).

(1) A telecommunications carrier may use, disclose, or permit access to CPNI, without customer approval, in its provision of inside wiring installation, maintenance, and repair services.

(2) CMRS providers may use, disclose, or permit access to CPNI for the purpose of conducting research on the health effects of CMRS.

(3) LECs, CMRS providers, and entities that provide interconnected VoIP service as that term is defined in §9.3 of this chapter, may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, 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.

(d) A telecommunications carrier may use, disclose, or permit access to CPNI to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

[63 FR 20338, Apr. 24, 1998, as amended at 64 FR 53264, Oct. 1, 1999; 67 FR 59211, Sept. 20, 2002; 72 FR 31962, June 8, 2007]

§ 64.2007 Approval required for use of customer proprietary network information.

(a) A telecommunications carrier may obtain approval through written, oral or electronic methods.

(1) A telecommunications carrier relying on oral approval shall bear the burden of demonstrating that such approval has been given in compliance with the Commission's rules in this part.

(2) Approval or disapproval to use, disclose, or permit access to a customer's CPNI obtained by a telecommunications carrier must remain in effect until the customer revokes or limits such approval or disapproval.

(3) A telecommunications carrier must maintain records of approval, whether oral, written or electronic, for at least one year.

(b) *Use of Opt-Out and Opt-In Approval Processes.* A telecommunications carrier may, subject to opt-out approval or opt-in approval, use its customer's individually identifiable CPNI for the purpose of marketing communications-related services to that customer. A telecommunications carrier may, subject to opt-out approval or opt-in approval, disclose its customer's individually identifiable CPNI, for the purpose of marketing communications-related services to that customer, to its agents and its affiliates that provide communications-related services. A telecommunications carrier may also permit such persons or entities to obtain access to such CPNI for such purposes. Except for use and disclosure of CPNI that is permitted without customer approval under section §64.2005, or that is described in this paragraph, or as otherwise provided in section 222 of the Communications Act of 1934, as amended, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

[67 FR 59212, Sept. 20, 2002, as amended at 71 FR 31962, June 8, 2007]

§ 64.2008 Notice required for use of customer proprietary network information.

(a) *Notification, Generally.* (1) Prior to any solicitation for customer approval, a telecommunications carrier must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

(2) A telecommunications carrier must maintain records of notification, whether oral, written or electronic, for at least one year.

(b) Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI.

(c) *Content of Notice.* Customer notification must provide sufficient information to enable the customer to make an informed decision as to whether to permit a carrier to use, disclose, or permit access to, the customer's CPNI.

(1) The notification must state that the customer has a right, and the carrier has a duty, under federal law, to protect the confidentiality of CPNI.

(2) The notification must specify the types of information that constitute CPNI and the specific entities that will receive the CPNI, describe the purposes for which CPNI will be used, and inform the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time.

(3) The notification must advise the customer of the precise steps the customer must take in order to grant or 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. However, carriers may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

(4) The notification must be comprehensible and must not be misleading.

(5) If written notification is provided, the notice must be clearly legible, use sufficiently large type, and be placed in an area so as to be readily apparent to a customer.

(6) If any portion of a notification is translated into another language, then all portions of the notification must be translated into that language.

(7) A carrier may state in the notification that the customer's approval to use CPNI may enhance the carrier's ability to offer products and services tailored to the customer's needs. A carrier also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

(8) A carrier may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

(9) The notification must state that any approval, or denial of approval for the use of CPNI outside of the service to which the customer already subscribes from that carrier is valid until the customer affirmatively revokes or limits such approval or denial.

(10) A telecommunications carrier's solicitation for approval must be proximate to the notification of a customer's CPNI rights.

(d) *Notice Requirements Specific to Opt-Out.* A telecommunications carrier must provide notification to obtain opt-out approval through electronic or written methods, but not by oral communication (except as provided in paragraph (f) of this section). The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(1) Carriers must wait a 30-day minimum period of time after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI. A carrier may, in its

discretion, provide for a longer period. Carriers must notify customers as to the applicable waiting period for a response before approval is assumed.

(i) In the case of an electronic form of notification, the waiting period shall begin to run from the date on which the notification was sent; and

(ii) In the case of notification by mail, the waiting period shall begin to run on the third day following the date that the notification was mailed.

(2) Carriers using the opt-out mechanism must provide notices to their customers every two years.

(3) Telecommunications carriers that use e-mail to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notification:

(i) Carriers must obtain express, verifiable, prior approval from consumers to send notices via e-mail regarding their service in general, or CPNI in particular;

(ii) Carriers must allow customers to reply directly to e-mails containing CPNI notices in order to opt-out;

(iii) Opt-out e-mail notices that are returned to the carrier as undeliverable must be sent to the customer in another form before carriers may consider the customer to have received notice;

(iv) Carriers that use e-mail to send CPNI notices must ensure that the subject line of the message clearly and accurately identifies the subject matter of the e-mail; and

(v) Telecommunications carriers must make available to every customer a method to opt-out that is of no additional cost to the customer and that is available 24 hours a day, seven days a week. Carriers may satisfy this requirement through a combination of methods, so long as all customers have the ability to opt-out at no cost and are able to effectuate that choice whenever they choose.

(e) *Notice Requirements Specific to Opt-In.* A telecommunications carrier may provide notification to obtain opt-in approval through oral, written, or electronic methods. The contents of any such notification must comply with the requirements of paragraph (c) of this section.

(f) *Notice Requirements Specific to One-Time Use of CPNI.* (1) Carriers may use oral notice to obtain limited, one-time use of CPNI for inbound and outbound customer telephone contacts for the duration of the call, regardless of whether carriers use opt-out or opt-in approval based on the nature of the contact.

(2) The contents of any such notification must comply with the requirements of paragraph (c) of this section, except that telecommunications carriers may omit any of the following notice provisions if not relevant to the limited use for which the carrier seeks CPNI:

(i) Carriers need not advise customers that if they have opted-out previously, no action is needed to maintain the opt-out election;

(ii) Carriers need not advise customers that they may share CPNI with their affiliates or third parties and need not name those entities, if the limited CPNI usage will not result in use by, or disclosure to, an affiliate or third party;

(iii) Carriers need not disclose the means by which a customer can deny or withdraw future access to CPNI, so long as carriers explain to customers that the scope of the approval the carrier seeks is limited to one-time use; and

(iv) Carriers may omit disclosure of the precise steps a customer must take in order to grant or deny access to CPNI, as long as the carrier clearly communicates that the customer can deny access to his CPNI for the call.

[67 FR 59212, Sept. 20, 2002]

§ 64.2009 Safeguards required for use of customer proprietary network information.

- (a) Telecommunications carriers must implement a system by which the status of a customer's CPNI approval can be clearly established prior to the use of CPNI.
- (b) Telecommunications carriers must train their personnel as to when they are and are not authorized to use CPNI, and carriers must have an express disciplinary process in place.
- (c) All carriers shall maintain a record, electronically or in some other manner, of their own and their affiliates' sales and marketing campaigns that use their customers' CPNI. All carriers shall maintain a record of all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record must include a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as a part of the campaign. Carriers shall retain the record for a minimum of one year.
- (d) Telecommunications carriers must establish a supervisory review process regarding carrier compliance with the rules in this subpart for outbound marketing situations and maintain records of carrier compliance for a minimum period of one year. Specifically, sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval.
- (e) A telecommunications carrier must have an officer, as an agent of the carrier, sign and file with the Commission a compliance certificate on an annual basis. The officer must state in the certification that he or she has personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the rules in this subpart. The carrier must provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the rules in this subpart. In addition, the carrier must 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. This filing must be made annually with the Enforcement Bureau on or before March 1 in EB Docket No. 06-36, for data pertaining to the previous calendar year.
- (f) Carriers must provide written notice within five business days to the Commission of any instance where the opt-out mechanisms do not work properly, to such a degree that consumers' inability to opt-out is more than an anomaly.
- (1) The notice shall be in the form of a letter, and shall include the carrier's name, a description of the opt-out mechanism(s) used, the problem(s) experienced, the remedy proposed and when it will be/was implemented, whether the relevant state commission(s) has been notified and whether it has taken any action, a copy of the notice provided to customers, and contact information.
- (2) Such notice must be submitted even if the carrier offers other methods by which consumers may opt-out.

[63 FR 20338, Apr. 24, 1998, as amended at 64 FR 53264, Oct. 1, 1999; 67 FR 59213, Sept. 20, 2002; 72 FR 31962, June 8, 2007]

§ 64.2010 Safeguards on the disclosure of customer proprietary network information.

- (a) *Safeguarding CPNI.* Telecommunications carriers must take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Telecommunications carriers must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, online account access, or an in-store visit.
- (b) *Telephone access to CPNI.* Telecommunications carriers may only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides the carrier with a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, the

telecommunications carrier may only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to the telecommunications carrier during a customer-initiated call without the telecommunications carrier's assistance, then the telecommunications carrier is permitted to discuss the call detail information provided by the customer.

(c) *Online access to CPNI.* A telecommunications carrier must authenticate a customer without the use of readily available biographical information, or account information, prior to allowing the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password, as described in paragraph (e) of this section, that is not prompted by the carrier asking for readily available biographical information, or account information.

(d) *In-store access to CPNI.* A telecommunications carrier may disclose CPNI to a customer who, at a carrier's retail location, first presents to the telecommunications carrier or its agent a valid photo ID matching the customer's account information.

(e) *Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords.* To establish a password, a telecommunications carrier must authenticate the customer without the use of readily available biographical information, or account information. Telecommunications carriers may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(f) *Notification of account changes.* Telecommunications carriers must notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification is not required when the customer initiates service, including the selection of a password at service initiation. This notification may be through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record, and must not reveal the changed information or be sent to the new account information.

(g) *Business customer exemption.* Telecommunications carriers may bind themselves contractually to authentication regimes other than those described in this section for services they provide to their business customers that have both a dedicated account representative and a contract that specifically addresses the carriers' protection of CPNI.

[72 FR 31962, June 8, 2007]

§ 64.2011 Notification of customer proprietary network information security breaches.

(a) A telecommunications carrier shall notify law enforcement of a breach of its customers' CPNI as provided in this section. The carrier shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or these rules, until it has completed the process of notifying law enforcement pursuant to paragraph (b) of this section.

(b) As soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, the telecommunications carrier shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through a central reporting facility. The Commission will maintain a link to the reporting facility at <http://www.fcc.gov/eb/cpni>.

(1) Notwithstanding any state law to the contrary, the carrier shall not notify customers or disclose the breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided in paragraphs (b)(2) and (b)(3) of this section.

(2) If the carrier believes that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed under paragraph (b)(1) of this section, in order to avoid immediate and irreparable harm, it shall so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency. The carrier shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(3) If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, such agency may direct the carrier not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency shall notify the carrier when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to the carrier, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers.

(c) *Customer notification.* After a telecommunications carrier has completed the process of notifying law enforcement pursuant to paragraph (b) of this section, it shall notify its customers of a breach of those customers' CPNI.

(d) *Recordkeeping.* All carriers shall maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to paragraph (b) of this section, and notifications made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. Carriers shall retain the record for a minimum of 2 years.

(e) *Definitions.* As used in this section, a "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.

(f) This section does not supersede any statute, regulation, order, or interpretation in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this section, and then only to the extent of the inconsistency.

[72 FR 31963, June 8, 2007]