



ITI CPNI Compliance Officer Manual

I. What is CPNI?

Customer proprietary network information (CPNI)

Information that relates to the quantity, technical configuration, type, destination, location, 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 Information contained in the bills pertaining to telephone exchange service or telephone toll service received by a Customer of a Carrier.

Examples:

- o Information regarding to whom, where, and when a Customer places a call;
- o Frequency, timing, and duration of calls;
- o The types of service offerings to which the Customer subscribes;
- o The extent to which a Customer uses a service;
- o The Customer's pre-subscribed toll provider; and
- o Call Detail Information on Inbound and Outbound Calls.

II. Why CPNI?

To Protect private information of customers of telecommunications carriers and interconnected Voice over Internet Protocol (VoIP) service providers

Congress recognized both that telecommunications carriers are in a unique position to collect sensitive personal information – including to whom, where and when their customers call – and that customers maintain an important privacy interest in protecting this information from disclosure and dissemination. Accordingly, section 222 of the Communications Act, 47 U.S.C. § 222, requires telecommunications carriers (and interconnected VoIP service providers) to take specific steps to

ensure that customer proprietary network information (CPNI) is adequately protected from unauthorized disclosure.

International Telecom Inc. (ITI) policy to comply with CPNI

The Company's policy is to protect the confidentiality of CPNI, and to rely on the involvement of high-level management to ensure that no use of CPNI is made until a full review of applicable law has occurred.

The FCC's regulations, 47 CFR 64.2009, require the Company to implement a system to clearly establish the status of a Customer's CPNI approval prior to the use of CPNI, and to train its personnel as to when they are, and are not, authorized to use CPNI, and to have an express disciplinary process in place. This Manual constitutes the Company's policies and procedures related to CPNI. All employees are required to follow the policies and procedures specified in this Manual.

III. ITI Policy regarding CPNI handling by employees.

ITI and its employees are prohibited from sharing customer's information to any other third party. ITI does not provide customers with ability to view their invoices over the internet using a login username and password. Since 1991 thru today, ITI has not, nor intends sell or allow data brokers information to our client's database. ITI customers database are strictly for ITI use only. Anyone caught sharing of database information by any employee will be reported to law enforcement, the FBI and United States Secret Service.

IV. EMPLOYEE COMPLIANCE REQUIREMENTS

A. Rule Requirements

Safeguarding CPNI

All employees must keep all customer information private to those customers whom have verified by user password to access to customer information

As the Compliance Officer you are responsible to report any unauthorized access to CPNI to the appropriate legal authorities.

All employees must properly authenticate a customer prior to disclosing CPNI based on customer-initiated telephone contact, access, or an in-store visit. [47 C.F.R. § 64.2010(a)]

Password for online access to CPNI

ITI does not provide this service to allow online access to their accounts.

Should ITI in future provide this service, these procedures must be followed:

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 that is not prompted by the carrier asking for readily available biographical information, or account information. [47 C.F.R. § 64.2010(c)]

Establishing a password

To establish a password, ITI must authenticate the customer without the use of readily available biographical information, or account information.

ITI 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. [47 C.F.R. § 64.2010(e)]

Password for telephone access to call detail information

All ITI employee's 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** that is not prompted by you asking for readily available biographical information, or account information.

If the customer does not provide a password, you 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 or asking for the answer to their back-up secret question(s).

If the customer is able to provide call detail information to you during a customer-initiated call without your assistance, then you are permitted to discuss the call detail information provided by the customer. [47C.F.R. § 64.2010(b)]

In-store access to CPNI

Employees may disclose CPNI to a customer who visits ITI's retail location, first presents to you with a valid photo ID matching the customer's account information. [47 C.F.R. § 64.2010(d)]

Opt-in/opt-out customer approval

ITI policy does not permit sharing of customer data to any company or entity, however if in the future should ITI elect to you must follow these Opt-in/opt out procedures.

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, or as otherwise described in section 64.2007(b) or otherwise provided in section 222, a telecommunications carrier may only use, disclose, or permit access to its customer's individually identifiable CPNI subject to opt-in approval.

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

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.

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. [47 C.F.R. § 64.2007]

Training and express disciplinary process in place

ITI and its employees are prohibited from sharing customer's information to any other third party. ITI does not provide customers with ability to view their invoices over the internet using a login username and password. Since 1991 thru today, ITI has not, nor intends to sell or allow data brokers information to our client's database in the future. ITI customers database are strictly for ITI use only. Anyone caught sharing of database information by any employee will be reported to law enforcement, the FBI and United States Secret Service.

Every employee must read the CPNI Employee manual and pass a verbal Q&A test.

Should any employee use CPNI unlawfully, they will be placed on leave of absence without pay for 5 days until a full investigation can be complete by the Compliance Officer, FBI and USSS. [47 C.F.R. § 64.2009(b)]

Notification Requirements

SUSPECTED BREACH OF CPNI

You must notify the Compliance Officer immediately of suspected breach of CPNI information. You shall notify the Compliance Officer immediately if a customer informs you of suspected breach of CPNI. The Compliance Officer will then contact law enforcement of a breach of its customers' CPNI. The Compliance Officer shall not notify its customers or disclose the breach publicly, whether voluntarily or under state or local law or the Commission's rules, until it has completed the process of notifying law enforcement.

As soon as practicable, and in no event later than **seven business days**, after reasonable determination of the breach, ITI 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>.

Notwithstanding any state law to the contrary, ITI shall not notify customers or disclose the breach to the public until **seven full business days** have passed after notification to the USSS and the FBI, except as provided below.

If you believe that there is an extraordinarily urgent need to notify any class of affected customers sooner than otherwise allowed, 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.

You will cooperate with the relevant investigating.

You will cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

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 ITI 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. **[47 C.F.R. § 64.2011(a)-(b)]**

Notification to customer of breach

After you have completed the process of notifying law enforcement, you notify its customers of a breach of those customers' CPNI. **[47 C.F.R. § 64.2011(c)]**

Notification of account changes

You 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 an 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. [47 C.F.R. § 64.2010(f)]

Notification before use of CPNI

Notification generally

Prior to any solicitation for customer approval, ITI must provide notification to the customer of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI. Individual notice to customers must be provided when soliciting approval to use, disclose, or permit access to customers' CPNI. [47 C.F.R. §64.2008]

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.

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.

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.

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, ITI may provide a brief statement, in clear and neutral language, describing consequences directly resulting from the lack of access to CPNI.

The notification must be comprehensible and must not be misleading.

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.

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

ITI 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.

ITI also may state in the notification that it may be compelled to disclose CPNI to any person upon affirmative written request by the customer.

ITI may not include in the notification any statement attempting to encourage a customer to freeze third-party access to CPNI.

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.

ITI's solicitation for approval must be proximate to the notification of a customer's CPNI rights. **[47 C.F.R. § 64.2008]**

Notice Requirements Specific to Opt-Out

ITI must provide notification to obtain opt-out approval through **electronic** or **written** methods, but not by oral communication, except as allowed for notice requirements specific to onetime use of CPNI.

If ITI uses the opt-out mechanism must provide notices to their customers **every two years**.

Waiting periods:

ITI must wait for a minimum of 30 days after giving customers notice and an opportunity to opt-out before assuming customer approval to use, disclose, or permit access to CPNI.

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

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

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.

E-mail notifications:

Should ITI use **e-mail** to provide opt-out notices must comply with the following requirements in addition to the requirements generally applicable to notification:

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

ITI must allow customers to reply directly to emails containing CPNI notices in order **to opt-out**;

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;

If ITI uses 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

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**

ITI 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. [47 C.F.R. § 64.2008]

Notice Requirements Specific to Opt-In

ITI may provide notification to obtain opt-in approval through oral, written, or electronic methods. [47 C.F.R. § 64.2008]

Notice Requirements Specific to One-Time Use of CPNI

ITI 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.

The contents of any such notification must comply with the content of notice requirements, 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:

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

ITI 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;

ITI 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

ITI 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. [47 C.F.R. § 64.2008]

Recordkeeping Requirements

Records related to breaches

ITI will maintain a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI, 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.

ITI shall retain the record for a minimum of **two years**. [47 C.F.R. § 64.2011(d)]

Records of approval

ITI will maintain records of customer approval for use of CPNI, whether oral, written, or electronic, for at least **one year**. [47 C.F.R. § 64.2007(a)(3)]

Records of notification

ITI will maintain records of customer notification of the customers' right to restrict use of CPNI, whether oral, written, or electronic, for at least **one year**. [47 C.F.R. § 64.2008(a)(2)]

Records of marketing campaigns using CPNI

ITI will 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.

ITI shall retain the record for a minimum of **one year**. [47 C.F.R. § 64.2009(c)]

Records of supervisory review process

ITI has established Joseph J Fetko as ITI's CPNI Compliance Officer. The CPNI Compliance Officer will be responsible for reviewing processes regarding carrier compliance with the rules 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. [47 C.F.R. § 64.2009(d)]

Filing Requirements

Compliance certification – March 1 (annually)

ITI will 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 Commission's CPNI rules.

ITI will provide a statement accompanying the certificate explaining how its operating procedures ensure that it is or is not in compliance with the Commission's CPNI rules. [47 C.F.R. § 64.2009(e)]

ITI will include an explanation of any actions taken against data brokers; and

ITI will report on proceedings instituted or petitions filed by a carrier at either state commissions, the court system, or at the Commission against data brokers. **[EPIC CPNI Order]**

A summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. **[47 C.F.R. § 64.2009(e)]**

For the summary of customer complaints, ITI must report on the number of customer complaints a carrier has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category of complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information.

ITI will also report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps carriers are taking to protect CPNI. **[EPIC CPNI Order]**

Any violation of, or departure from, the policies and procedures in this Manual shall be reported immediately to Joseph J Fetko the ITI Compliance Officer at (907)349-6557.

V. DEFINITIONS

§ 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.