



## The *Comm*Law Group

HELEIN & MARASHLIAN, LLC  
1483 Chain Bridge Road  
Suite 301  
McLean, Virginia 22101

Telephone: (703) 714-1300  
Facsimile: (703) 714-1330  
E-mail: [mail@CommLawGroup.com](mailto:mail@CommLawGroup.com)  
Website: [www.CommLawGroup.com](http://www.CommLawGroup.com)

Writer's Direct Dial Number  
703-714-1313

Writer's E-mail Address  
[jsm@commlawgroup.com](mailto:jsm@commlawgroup.com)

February 25, 2010

### VIA ECFS TRANSMISSION

Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 – 12<sup>th</sup> Street, S.W.  
Suite TW-A325  
Washington, D.C. 20554

Re: *Apptix, Inc.*  
*Annual 47 C.F.R. §64.2009(e) Certification*  
*EB Docket No. 06-36*

Dear Ms. Dortch:

Enclosed herewith for filing with the Federal Communications Commission in the above-referenced docket is the Annual §64.2009(e) CPNI Certification and supporting statement of Apptix, Inc.

Although Apptix does provide VoIP services, the company does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. Furthermore, the Company has taken significant steps to develop and implement operational safeguards to maintain the confidentiality of CPNI. Indeed, Apptix continually updates and revises its CPNI Compliance Policies and Procedures to continually strengthen existing safeguards and to accommodate periodic modifications to the FCC's rules and regulations.

The Company has made a business decision that CPNI will not be utilized, and has established procedures and put safeguards in place to protect against inadvertent disclosure of CPNI. Furthermore, Apptix has experienced no customer complaints concerning the unauthorized use of CPNI and has not taken any actions against data brokers. Through filing, the Commission is now fully apprised of the measures which Apptix has adopted to ensure the ongoing protection of

CPNI and the Company's commitment to continued compliance with the FCC's CPNI rules and regulations.

Attached hereto is a "public" version of Apptix's currently effective CPNI policy document. This document has been redacted to remove information considered confidential and proprietary by the Company. Apptix will make a non-redacted version of the attached CPNI Certification to the Commission upon request and under seal.

To the extent you have any questions concerning this filing, please contact the undersigned.

Respectfully submitted,

/s/

Jonathan S. Marashlian  
Attorney for Apptix, Inc.

# Apptix, Inc.

Annual CPNI Certification  
47 C.F.R. §64.2009(e)  
EB Docket No. 06-36

**COMPANY NAME:** Apptix, Inc.

**FILER ID:** 826640

**OFFICER:** Christopher E. Mack

**TITLE:** Chief Financial Officer

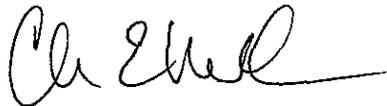
I certify that I am an officer of the company named above and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Federal Communication Commission's CPNI rules. *See 47 C.F.R. §64.2001 et seq.*

Attached to this certification is the company's CPNI Compliance Certification Policies and Procedures Manual. This Manual explains how the company ensures compliance with all the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

Apptix has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission) against data brokers in the past year. The company has no information to report with respect to the processes pretexters are using to attempt to access CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized use of CPNI.

Signed:



On behalf of Apptix, Inc.

Date:

2-22-2010

---

# **CPNI Compliance Certification Policies and Procedures**

**for**

**Apptix**

**Version 1.6**

**Prepared by John Kersse**

**February 09, 2010**

# Table of Contents

- Table of Contents ..... ii**
- 1. Introduction.....1**
  - 1.1 Purpose ..... 1
  - 1.2 Use of CPNI ..... 1
- 2. Storage of CPNI .....1**
- 3. Sales and Marketing .....2**
  - 3.1 Campaign Approval and Supervisory Review ..... 2
    - 3.1.1 Statement on CPNI Usage..... 2
    - 3.1.2 Sales ..... 2
    - 3.1.3 Marketing ..... 2
  - 3.2 Opt-In ..... 3
    - 3.2.1 Customer Opt-In Notification ..... 3
    - 3.2.2 Confidentiality..... 3
  - 3.3 Opt-Out Mechanism Failure ..... 3
  - 3.4 Opt-Out Failure Record Keeping ..... 3
    - 3.4.1 System Description ..... 3
    - 3.4.2 System Storage..... 3
- 4. Employee Training and Discipline .....4**
- 5. Customer Authentication Methods .....4**
  - 5.1 Statement of Business Customer Exemption..... 4
  - 5.2 Process to Access to CPNI via Download..... 4
    - 5.2.1 Password Management..... 5
- 6. Customer Notification of CPNI Changes.....5**
- 7. Notification to Law Enforcement and Customers of Unauthorized Access .....5**
  - 7.1 Notifications ..... 5
    - 7.1.1 Law Enforcement ..... 5
    - 7.1.2 Customer ..... 5
  - 7.2 Unauthorized Access Record Keeping ..... 5
    - 7.2.1 System Description ..... 5
    - 7.2.2 System Storage..... 6
- 8. Appendix A .....7**
  - 8.1 Aptix Policy on the Protection of Customer Proprietary Network Information (CPNI) ..... 7

## Revision History

[NOT FOR PUBLIC DISCLOSURE IN EB DOCKET NO. 06-36]

# 1. Introduction

## 1.1 Purpose

Under Federal law, Customer Proprietary Network Information (CPNI) is certain customer information obtained by a telecommunications provider during the course of providing service to the customer. This includes information relating 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. CPNI may also include information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

This document will detail the processes and procedures that to which Apptix employees will adhere when working with CPNI.

## 1.2 Use of CPNI

It is the policy of Apptix not to use CPNI for any activity other than as permitted by applicable law. Any disclosure of CPNI to other parties (such as affiliates, vendors and agents) occurs only if it is necessary to conduct a legitimate business activity related to the services already provided by Apptix to the customer. If Apptix is not required by law to disclose CPNI or if the intended use is not otherwise permitted under FCC Rules, the company will first obtain the customer's consent prior to using or sharing CPNI.

# 2. Storage of CPNI

Except as permitted by 47 C.F.R. § 64.2005(a), (c) and (d), Apptix uses CPNI only for the purposes of billing customers for usage-based services and as necessary to assist customers in the resolution of service issues. Call detail records (CDRs) are processed and rated by a third-party billing provider, presently . Apptix has entered into appropriate agreements with pursuant to the billing provider has committed to protect the confidentiality of Apptix customer CPNI. Each month, Apptix receives full CPNI/CDR data from our third party billing provider, , which is then imported into the Voice Billing database. These imports are then converted into "readable" CDR records and the original import files from are purged every 90 days.

The external, outsourced, billing system can be accessed with a user ID and password. Only two people can access the system at any one time. Access is limited to provisioning and support personnel.

Internal billing system CDR data is secured on a Microsoft SQL Server Database by username/password. Access to this system is limited to Management, Operations personnel who perform backups and maintenance of these databases and Programming Personnel who perform monthly data imports from the third party billing provider.

Apptix stores one of two types of CPNI data for each VoIP customer:

1. Full CDR – All call detail records for all usage types

2. Billable CDR – A subset of call detail records for International, certain long distance and toll free usage.

By default, Apptix retains only Billable CDR data unless the customer requests that we store Full CDR data. If a customer has provided us express direction, we will make Full CDRs available via a secure, password-protected download mechanism. Customers can view CDR data for a period of 90 days.

## **3. Sales and Marketing**

### **3.1 Campaign Approval and Supervisory Review**

All sales and marketing campaigns are approved by management.

#### **3.1.1 Statement on CPNI Usage**

Except as provided by 47 C.F.R. §64.2005 and as otherwise permitted by Federal Communications Commission Rules, Apptix does not use CPNI in customer marketing efforts. All customer marketing communications are based upon a master customer database that is comprised of non-CPNI information. This database stores customer contact information and details on the service packages that have been purchased by the customer.

#### **3.1.2 Sales**

Sales personnel do not have access to CPNI.

#### **3.1.3 Marketing**

All marketing campaigns are reviewed by the Vice President of Marketing, the product management team and finally, Apptix Legal team prior to execution. Except as provided by 47 C.F.R. §64.2005 and as otherwise permitted by Federal Communications Commission Rules, CPNI information is not used for customer marketing campaigns.

## **3.2 Opt-In**

Apptix does not disclose CPNI to agents, affiliates, joint venture partners, independent contractors or to any other third parties to for marketing purposes.

In the event that Apptix were to change this policy, the following steps would be taken to ensure that customers are notified of the intension to use CPNI for this purpose and to get specific customer authorization to do so.

### **3.2.1 Customer Opt-In Notification**

1. Notification to primary contact on record via Email and stating policy change.
  - a. Opt-in Notification will advise the customer of a specific URL or email address where they can opt-in or deny access to their CPNI.
  - b. Opt-In preference information will be stored in the main customer database.
2. Joint Marketing campaigns utilizing CPNI will only be sent to those customers who have been flagged in the customer database as CPNI Opt-In.
3. Customer will have the ability to access the URL or email address at any time to change their preference.
  - a. Preference will be updated within the main customer database within X period of time.

### **3.2.2 Confidentiality**

Prior to releasing customer Opt-in CPNI information, any joint venture partners, independent contractors or other third parties will be required to sign an Apptix Mutual Confidentiality and Non-Disclosure Agreement.

## **3.3 Opt-Out Mechanism Failure**

In the event that Apptix determines that an opt-out mechanism is not working properly, Apptix will send an overnight, certified letter within five (5) days to the Secretary of the FCC and have that letter directed to CC Docket No. 96-115 with details on what mechanism failed and what actions were taken to ensure that a similar failure will not reoccur.

## **3.4 Opt-Out Failure Record Keeping**

### **3.4.1 System Description**

A record of each CPNI marketing campaign will be saved in an Excel spreadsheet. Additional information on marketing campaigns may also potentially be stored in an Apptix CRM database.

Each record will contain a description of each campaign, the specific CPNI that was used in the campaign, what products and services were offered as a part of the campaign and the names of affiliates and independent contractors that were involved in the offer.

### **3.4.2 System Storage**

This spreadsheet will be maintained on a secure, Aptix Site for a minimum of one (1) year. This site is backed up daily to ensure data security and integrity.

## **4. Employee Training and Discipline**

All Aptix employees participate in a new hire orientation with a member of the Human Resources department. During this orientation employees that will have contact with CPNI will receive additional training on CPNI and how it is their responsibility to protect it. Employees will be required to sign the Aptix Policy on the Protection of Customer Proprietary Network Information (CPNI) (see Appendix A) stating that they have received CPNI training and that they understand and acknowledge the duty to protect confidential information specifically extends to the protection of Customer Proprietary Network Information (CPNI) and agree to fully comply with the Company's rules and regulations for the protection and permissible use thereof.

Any violation of this policy is subject to disciplinary action up to and including dismissal.

Participation in Aptix' CPNI training will not be limited to employees whose job functions bring them into contact with CPNI on a routine basis. CPNI training will be available to any requesting Aptix employee. In addition, a copy of Aptix' CPNI policies, procedures and CPNI training materials will be maintained by the Human Resources department for review by any requesting employee. The Company is fully committed to ensuring the protection of customer CPNI. Aptix advises all employees, even those not likely to come into contact with CPNI as part of their routine job functions, of the necessity to protect CPN. All Aptix employees are subject to the Company's CPNI policies and regulations, including disciplinary action, regardless of whether contact with CPNI occurs during performance of normal job functions or inadvertently.

## **5. Customer Authentication Methods**

### **5.1 Statement of Business Customer Exemption**

Aptix provides Voice over Internet Protocol (VoIP) services to business customers only. Based on this business to business relationship, Aptix is exempt from the "Customer Authentication Methods" requirements pertaining to Authorized Disclosure of CPNI. Our customers (1) Have established privacy protections in contracts with Aptix; and (2) Are served by a dedicated account team with a specified team lead.

### **5.2 Process to Access to CPNI via Download**

From time to time, customers may request raw call detail information so that they can create their own reports. Customers who wish to view the details of their CDR data can do so by requesting a password to the section of the web site.

Customers can then log into this section of the website and view their billing information and past invoices for the past 90 days. For all VoIP invoices that contain CDR charges, there is a download link that will allow the customer to download a CSV (comma separated text file) file to view their CDR data.

### **5.2.1 Password Management**

Because the \_\_\_\_\_ section is tightly integrated with the \_\_\_\_\_ product, the customer can change their password by logging into \_\_\_\_\_ (a link is provided in the \_\_\_\_\_ Section) with their current username and password. There is an option in \_\_\_\_\_ that will allow the customer to privately change their password. Customers can also request a new password by contacting our support department and we can facilitate this for the customer.

## **6. Customer Notification of CPNI Changes**

All customer notifications regarding account changes will be sent by email to the email address of the primary contact on record.

## **7. Notification to Law Enforcement and Customers of Unauthorized Access**

### **7.1 Notifications**

#### **7.1.1 Law Enforcement**

In the event that Apptix discovers that a CPNI breach has occurred, Apptix will notify The United States Secret Service and the Federal Bureau of Investigation through the Data Breach Reporting Portal at <https://www.cpnireporting.gov/dtrp/content/disclaimer.faces> within seven (7) days of the discovery.

Notwithstanding the above, Apptix may not wait the additional seven (7) days to notify its customers if the company determines there is an immediate risk of irreparable harm to the customers. Apptix shall cooperate with the relevant law enforcement agency to minimize any adverse effects of such customer notification.

#### **7.1.2 Customer**

Except in cases where Apptix is directed by an appropriate law enforcement agency to refrain from, or delay, customer notification of a CPNI breach, in the event that Apptix discovers that a CPNI breach has occurred, Apptix will notify the affected customer(s) by sending an email to the primary contact's email address on record detailing the specifics of the breach and what steps have been taken to ensure a similar breach will not reoccur. If Apptix receives notification that the email could not be successfully delivered through a Non-Delivery Record or other bounce message, the primary contact on record will be contacted by telephone to the primary phone number on record.

### **7.2 Unauthorized Access Record Keeping**

#### **7.2.1 System Description**

A record of any CPNI breach will be recorded in an Excel spreadsheet.

This spreadsheet will contain data on: (1) dates of discovery and notification, (2) detailed description of the CPNI that was the subject of the breach, and (3) the circumstances of the breach.

### **7.2.2 System Storage**

This spreadsheet will be stored and maintained on a secure, \_\_\_\_\_ Site for a minimum of two (2) years. This site is backed up daily to ensure data security and integrity.

## **8. Appendix A**

### **8.1 Apptix Policy on the Protection of Customer Proprietary Network Information (CPNI)**

**[NOT FOR PUBLIC DISCLOSURE IN EB DOCKET NO. 06-36]**