

LAWYERS



## Davis Wright Tremaine LLP

ANCHORAGE BELLEVUE LOS ANGELES NEW YORK PORTLAND SAN FRANCISCO SEATTLE SHANGHAI WASHINGTON, D.C.

PAUL HUDSON  
DIRECT (202) 973-4275  
paulhudson@dwt.com

SUITE 200  
1919 PENNSYLVANIA AVE NW  
WASHINGTON, DC 20006

TEL (202) 973-4200  
FAX (202) 973-4499  
www.dwt.com

February 29, 2008

### VIA ELECTRONIC FILING

Marlene H. Dortch  
Office of the Secretary,  
Federal Communications Commission  
445 12th Street, S.W.  
Washington, D. C. 20554

**Re: EB Docket 06-36, Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

Annual § 64.2009(e) CPNI Certification for 2007  
Date filed: February 29, 2008  
Name of company covered by this certification: **Access One, Inc.**  
Form 499 Filer ID: **819798**  
Name of signatory: **Mark Jozwiak**  
Title of signatory: **President**

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's Rules, 47 C.F.R. § 64.2009(e), enclosed for filing in the above-referenced docket is the executed annual CPNI Compliance Certificate of Access One, Inc.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'PBH', written over a light blue horizontal line.

Paul B. Hudson  
Counsel for Access One, Inc.

Enclosures

**CERTIFICATE OF COMPLIANCE**

**Annual 47 C.F.R. § 64.2009(e) CPNI Certification**

**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification for 2007

Date filed: February 29, 2008

Name of company covered by this certifications: **Access One, Inc.**

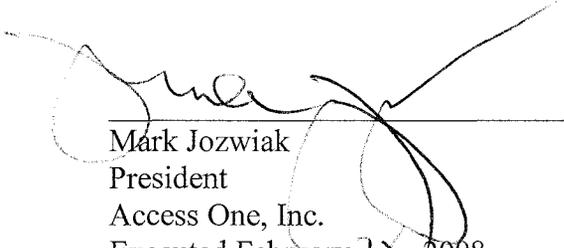
Form 499 Filer ID: **819798**

Name of signatory: **Mark Jozwiak**

Title of signatory: **President**

I, Mark Jozwiak, certify that I am an officer of Access One, Inc. ("Company") and, acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures, summarized in the attached statement, that are adequate to ensure compliance with the Commission's rules governing use and disclosure of confidential proprietary network information ("CPNI"), as governed by Section 222 of the Communications Act of 1934, as amended by the Telecommunications Act of 1996, and as set forth in Part 64, Subpart U of the of the Commission's rules, 47 C.F.R. §§ 64.2001 *et. seq.*

The Company has not received any customer complaints in the past calendar year concerning the unauthorized release of CPNI, and is not aware of any unauthorized disclosures of CPNI. Company does not have any material information with respect to the processes pretexters are using to attempt to access CPNI that is not already a part of the record in the Commission's CC Docket No. 96-115. Company has therefore not taken any actions against data brokers, including proceedings instituted or petitions filed by the Company at either state commissions, the court system or at the Commission. The Company has established procedures to report any future breaches to the FBI and United States Secret Service, and it has emphasized in its employee training of the need for vigilance in identifying and reporting unusual activity in order to enable the Company to continue to take reasonable measures to discover and protect against pretexting and other unauthorized access to CPNI.

  
\_\_\_\_\_  
Mark Jozwiak  
President  
Access One, Inc.  
Executed February 28, 2008

## **Revised CPNI Compliance Policies of Access One, Inc.**

Access One, Inc. (“Access One”) has implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information (“CPNI”) and to assure compliance with the rules of the Federal Communications Commission (“FCC”) set forth in 47 C.F.R. Part 64, Subpart U, Section 2001 *et seq.* Access One substantially revised its policies to implement the FCC’s new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, CC Docket No. 96-115, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007).

CPNI is “(A) 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 (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.”

Access One’s policy is administered by its CPNI Compliance Manager Jeff Sobek, General Counsel.

### **I. USE, DISCLOSURE OF, AND ACCESS TO CPNI**

Access One will use, disclose, or permit access to CPNI only as set forth herein.

#### **A. Use, Disclosure or Access to CPNI Without Customer Approval**

Access One may use, disclose and provide access to CPNI without customer approval in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for telecommunications services; to protect the rights or property of Access One, or to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to market services within the category or categories of services to which the customer already subscribes, including, for local exchange customers, 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), and, for local exchange or interexchange customers, to market CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store-and-forward, and protocol conversion services; to provide inside wiring installation, maintenance, or repair services; or as required by law (such as pursuant to a valid request from law enforcement or a court order or other appropriate authority).

#### **B. Customer Approval of Use, Disclosure and Access to CPNI**

Access One may use, disclose, or permit access to CPNI as expressly authorized by the customer.

Access One may use, or disclose or permit access, by its agents and affiliates that provide communications-related services, to a customer's individually identifiable CPNI to market to that customer any communications-related service offerings that are not within a category of service to which the customer already subscribes, but only with prior "opt-out" approval from the customer in accordance with the following procedures set forth in this section I.B.

A customer is deemed to have provided "opt-out" consent to such use, disclosure, or access to the customer's CPNI if the customer has failed to object thereto within 33 days following Access One's mailing of a comprehensible, non-misleading individual written notification that provides sufficient information to enable the customer to make an informed decision as to whether to permit Access One to use, disclose, or permit access to, the customer's CPNI, and that includes all of the following elements:

- prior to any solicitation for customer approval, explains that the customer has a right to restrict use of, disclosure of, and access to their CPNI, and that Access One has a duty, under federal law, to protect the confidentiality of CPNI;
- specifies the types of information that constitutes CPNI and the specific entities that will receive the CPNI;
- describes the purposes for which CPNI will be used;
- informs the customer of his or her right to disapprove those uses, and deny or withdraw access to CPNI at any time;
- advises the customer of the precise steps the customer must take in order to grant or deny access to CPNI;
- states clearly that a denial of approval will not affect the provision of any services to which the customer subscribes;
- is clearly legible, in sufficiently large type, and placed in an area so as to be readily apparent to a customer;
- does not include any statement encouraging a customer to freeze third-party access to CPNI;
- states 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, and that if the customer has opted-out previously, no action is needed to maintain their opt-out election; and
- states that customer's approval may be assumed by Access One if customer does not object to such use within 33 days of the mailing of the notice.

Access One makes available to every customer a method to opt-out that is of no additional cost to the customer and is available 24 hours a day, seven days a week.

Access One does not seek customer opt-out approval at any time that is not proximate to its provision of the above notification.

At this time, Access One does not provide notifications in languages other than English. If any part of a notification is translated into another language, all portions would be translated into that language.

Approval or disapproval to use, disclose, or permit access to a customer's CPNI shall remain in effect until the customer revokes or limits such approval or disapproval. However, to rely on a customer's prior out-out approval, Access One must provide a new notification to such customer every two years.

Access One may also use, disclose, or permit access to CPNI to provide inbound marketing, referral or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of the carrier's use to provide such service. In requesting such approval, the Company representative must explain that the customer has a right, and that Company has a duty, under federal law, to protect the confidentiality of CPNI; specifies the types of CPNI that would be used for the call and the purposes for which it would be used; informs the customer of his or her right to decline such use and that such denial will not affect the provision of any services to which the customer subscribes; and will not attempt to encourage a customer to freeze third-party access to CPNI.

### **C. Restrictions on Use of CPNI**

Access One does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers. For example, as a local exchange carrier, Access One does not use local service CPNI to track Customers that call local service competitors.

When Access One receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

## **II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES**

Access One will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Access One's existing policies that would strengthen protection of CPNI, they should report such information immediately to Access One's CPNI Compliance Manager so that Access One may evaluate whether existing policies should be supplemented or changed.

To prevent unauthorized access to CPNI, Access One employees must use a unique login and password to obtain access to databases that include CPNI, and CPNI is not routinely stored in paper form at Access One's offices.

Pursuant to 47 C.F.R. § 64.2010(g), the requirements of the FCC's authentication regime set forth in Section 64.2010 of its rules do not apply to business customer accounts that have both a dedicated account representative (who may be reached without going through a call center) and a contract with Access One that specifically addresses the carriers' protection of CPNI. Except as permitted by this business customer exemption, Access One does not disclose CPNI to any inbound telephone caller or any visitor to an Access One retail office. Access One does not provide online access to any account that provides access to CPNI, that is not subject to the business customer exemption.

Access One will notify customers immediately whenever a customer's password used to access CPNI, or online account is created or changed. When an address of record is created or changed, Access One will send a notice immediately to customer's former address of record notifying them of the change. These notifications are not required when the customer initiates service, including the selection of a password at service initiation. These notifications will be sent to customer's address of record, will not reveal the changed information, and will direct the customer to notify Access One immediately if they did not authorize the change.

### **III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT**

Any Access One employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the Access One CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Access One's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Access One's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

#### **A. Identifying a "Breach"**

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If an Access One employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must

be reported to Access One's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. Access One's CPNI Compliance Manager will determine whether it is appropriate to update Access One's CPNI policies or training materials in light of any new information; the FCC's rules require Access One on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

#### **B. Notification Procedures**

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the Access One CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: <https://www.cpnireporting.gov>. Access One's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or <http://www.fcc.gov/eb/cpni>) for instructions.

Access One will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI, except as provided below (a full business day does not count a business day on which the notice was provided).

If Access One receives no response from law enforcement after the 7<sup>th</sup> full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Access One will delay notification to customers or the public upon request of the FBI or USSS.

If the Access One Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Access One still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

#### **IV. RECORD RETENTION**

The CPNI Compliance Manager is responsible for assuring that Access One maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches 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.

Access One maintains a record, for a period of at least one year, of: (1) those limited circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI (pursuant to a valid request from law enforcement, court order or other appropriate authority); (2) of supervisory review of outbound marketing that proposes to use CPNI or to request customer approval to disclose CPNI; (3) its sales and marketing campaigns that use its customers' CPNI, including a description of each campaign, the specific CPNI that was used in the campaign, and the products and services offered as a part of the campaign; and (4) records associated with customers' "opt-out" approval or non-approval to use

CPNI, and of notification to customers prior to any solicitation for customer approval of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI.

Access One maintains a record of all customer complaints related to their handling of CPNI, and records of Access One's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that Access One considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Access One will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Access One has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Access One's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing 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. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

## **V. TRAINING**

Access One employees must use a unique login and password to obtain access to databases that include CPNI. All employees with such access receive a copy of Access One's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Access One requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.