February 1, 2010

Via Electronic Filing

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, DC 20554

RE: EB Docket No. 06-36
Annual CPNI Certification –Falcon1, Inc.

Dear Secretary Dortch:

On behalf of Falcon1, Inc. ("Falcon1"), enclosed for electronic filing is Falcon1's annual 64.2009(e) CPNI Certification for 2010 covering calendar year 2009. In accordance with the Consent Decree adopted August 5, 2009, Falcon1 is also submitting a copy of this certification to the Chief, Telecommunications Consumers Division, Enforcement Bureau.

Please contact the undersigned at 614.469.3294 or via email at Carolyn.Flahive@ThompsonHine.com if you have any questions regarding Falcon1's certification.

Thank you.

Very truly yours,

Carolyn S. Flahive

cc: Best Copy and Printing, Inc.,
via email – FCC@BCPIWEB.com

Chief, Telecommunications Consumers Division,
Enforcement Bureau, via FedEx

Paula McGraw, General Manager
Falcon1, Inc.

Enclosure

Carolyn.Flahive@ThompsonHine.com Phone 614.469.3294 Fax 614.469.3361 CSF/cjc 636588.1

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2010 covering the prior calendar year 2009

1. Date filed: February 1, 2010
2. Name of company(s) covered by this certification: Falcon1, Inc.
3. Form 499 Filer ID: 827045
4. Name of signatory: Joe Bennett
5. Title of signatory: President
6. Certification:

I, Joe Bennett, 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 Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

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

The company represents and warrants that the above certification is consistent with 47. C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed Joe Bennett

Attachments: Accompanying Statement explaining CPNI procedures

636129.1

FALCON1, INC.
STATEMENT OF CPNI PROCEDURES

Falcon1, Inc. ("Falcon1") is a wholly-owned subsidiary of Minford Telephone Company ("Minford"). Falcon1 has no employees. Rather, Minford personnel perform all functions related to the operations of Falcon1, including billing and customer service. Accordingly, the obligations to protect the customer proprietary network information ("CPNI") of Falcon1 customers are, in fact, fulfilled by employees of Minford.

Minford, and hence Falcon1, take the protection of CPNI very seriously. Minford maintains a CPNI Policy Handbook containing the following procedures that it has adopted to ensure the protection of CPNI. The handbook describes Minford's procedures in greater detail and provides practical guidance on how to protect against unauthorized disclosure or use of CPNI. The procedures contained in the handbook apply with respect to the seamless operations of both Minford and Falcon1. The handbook is distributed to Minford employees during training and serves as an important reference tool for Minford employees.

Duty to Protect CPNI

We recognize our duty to protect customer CPNI. We may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

1. Administrative use: We may use CPNI to *initiate, render, bill and collect* for communications services.

2. Protection of carrier and third parties: We may use CPNI to protect the interests of our company, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.

3. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

Our Own Use Of CPNI

We may use CPNI to provide or market services to our existing customers. We understand that we are required to obtain customer approval prior to using CPNI in certain ways.

Marketing

We understand that we do not need to obtain customer approval before using CPNI to market services to our existing customers within the categories of service to which the customer already subscribes.

We understand that we may not use CPNI to market services that are in a service category to which the customer does not already subscribe without customer approval.

We understand that we cannot use CPNI to solicit a customer to add a new category of service without first obtaining the customer's approval.

We know that we may not share CPNI with our affiliates unless we have obtained customer approval. We do not currently share CPNI with any third parties other than Minford, with whom we share our CPNI for billing and customer service purposes. This sharing falls under the administrative use exception and does not require prior customer approval.

We also understand that we do not need customer consent before using CPNI to market "adjunct-to-basic" services such as speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain centrex features.

We understand that we may not use CPNI to identify or track customers that call competing service providers.

We regularly review our marketing practices to determine when and how CPNI is used within the company, and whether CPNI is being shared with other entities. We also review new marketing or sales campaigns to ensure compliance with these CPNI policies and with the FCC's CPNI regulations.

Provision of Services

We understand that we do not need customer approval to use CPNI to provide CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

Authenticating Customers Before Disclosing CPNI

We understand that we are required to objectively determine that our customers are who they say they are before disclosing CPNI to them.

Telephone

We understand that when a customer calls, we may not release *call detail information*, or information relating to the transmission of specific telephone calls until we have obtained the account password from the caller, or called the customer back at the telephone number of record to ensure that the customer is who s/he says s/he is. Alternatively, we may offer to send the call detail information to the address of record or provide it to the customer or an authorized individual in person after s/he has produced valid photo identification at our office.

We understand that we may disclose *non-call detail information* over the telephone after authenticating the customer by calling back the telephone number of record, checking valid photo identification, or by mailing the information to the account address of record.

In-Person Authentication

We understand that before we can disclose CPNI to customers in person, the customer must present *valid government-issued photo identification*. The name on the photo identification must match the name on the account. If the customer cannot present the required identification, we offer to provide the requested CPNI by sending it to the account address of record.

Before providing the CPNI to the customer, we make a copy of the photo identification. This copy is then placed in the customer's file, together with a copy of the CPNI provided to the customer. These records are then kept in the customer file in accordance with our record-keeping policies.

Mail

If the customer requests CPNI through regular mail, or if the customer cannot comply with one of the authentication methods above, we send the requested information to the customer's address of record only.

Customer Notification of CPNI Rights

We provide a CPNI privacy policy to all customers annually, as a bill insert in the December bill. This policy provides notification to each customer of his/her right to restrict use of, disclosure of, and access to that customer's CPNI. We maintain a list of all customers who receive the privacy policy, the date on which the policy is sent, and a copy of the policy in our records for three (3) years following the mailing of the policy. We provide additional copies of the CPNI privacy policy to all customers who request it and to all new customers upon activation of service.

The policy contains an opt-out customer approval notice. Customers who do not wish to allow us to use their CPNI to market services outside their existing service categories, or who do not wish to allow us to share their CPNI with affiliates, have 30 days to contact us to tell us that they do not approve of this use. If we do not hear back from the customer within 30 days, we understand that we are free to use their CPNI for these purposes. We understand that customers can change their option at any time by contacting us, and we notify our customers of this right.

We maintain records of the customers who received the opt-out approval notice and records of the customers who contacted us to opt out in accordance with our record-keeping policies.

We understand that we must provide written notice to the FCC within five (5) business days if our opt-out mechanisms do not work properly to the degree that our customers' inability to opt out is more than an anomaly.

Training And Discipline

Minford's General Manager, Bookkeeper and Customer Service Representatives were trained regarding these CPNI policies prior to the effective date of the most recent CPNI regulations, December 8, 2007. These employees are required to attend an annual retraining to ensure that they understand these CPNI policies and any updates to these policies. New Minford employees who will have access to CPNI are trained when they are hired, and then attend the regularly-scheduled retraining sessions. At the conclusion of each training session, these employees are asked to sign certificates stating that they understand these CPNI policies and that they will comply with these policies.

We have implemented the following disciplinary guidelines for employees who fail to follow these CPNI policies:

> Minford Telephone Company has informed its employees that it considers compliance with the Communications Act and FCC rules regarding the use, disclosure, and access to CPNI to be very important.

Violation by employees of such CPNI requirements will lead to disciplinary action (including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether appropriate guidance was sought, and the extent to which the violation was or was not deliberate or malicious.

Disciplinary records are maintained in the company files in accordance with our record-keeping policies.

Record-Keeping

We maintain the following records in our files for three (3) years:

a. Records relating to the annual mailing of the customer CPNI privacy policy;

b. Records of customer approval or disapproval of CPNI use, or the limitation or revocation thereof;

c. Records of disclosure or provision of CPNI to third parties for marketing purposes, including Minford Telephone Company's and Falcon1's sales and marketing campaigns using customer CPNI, the CPNI used, and what products and services were offered as part of the campaign;

d. Employee disciplinary records; and

e. Records of discovered CPNI breaches, notifications to law enforcement regarding breaches, and any responses from law enforcement regarding those breaches.

Notification Of Account Changes

We understand that we are required to notify customers when changes have been made to passwords, customer responses to back-up means of authentication, or addresses of record by mailing a notification to the account address of record.

We do not reveal the changed account data in the notification.

Unauthorized Disclosure Of CPNI

We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at http://www.fcc.gov/eb/CPNI/ to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

Records relating to such notifications are kept in accordance with our record-keeping policies. These records include: (i) the date we discovered the breach, (ii) the date we notified law enforcement, (iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in

our annual CPNI compliance certification filed with the FCC.

Signed _____