



Jacquelyne Flemming
Asst. VP- Federal Regulatory

AT&T Services, Inc.
1120 20th Street, N.W.,
Suite 1000
Washington, D.C. 20036

202.457.3032 Phone
202.457.3071 Fax
jw1196@att.com E-mail

February 28, 2014

Via Electronic Submission

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
12th Street Lobby – TW-A325
Washington, D.C. 20554

**Re: AT&T Annual CPNI Compliance Certifications Calendar Year 2013
EB Docket No. 06-36**

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e), AT&T, on behalf of the attached list of operating entities, hereby submits its annual CPNI compliance certifications for calendar year 2013 via the Commission's Electronic Comment Filing System.

Should you have any questions, feel free to contact me.

Sincerely,

/s/ Jacquelyne Flemming
Jacquelyne Flemming

Attachment A – List of AT&T Operating Entities

Attachment B – Summary of Customer Complaints & Actions Taken Against Data Brokers

**AT&T Inc. CPNI Certification
Calendar Year 2013**

Date: 2-24-2014

1. I, Gerry R. Chicoine, SVP-Audit Services and Chief Compliance Officer, AT&T Services, Inc. Finance hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: 

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF Gerry R. Chicoine, SVP-Audit Services and Chief Compliance Officer, AT&T Services
Inc., Finance-Audit Services and Compliance**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by the Asset Protection, Credit & Collections, and Global Fraud Management organizations within AT&T Finance ensure compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals

1. The Credit and Collections organization has established methods and procedures to ensure compliance with the rules around approval for the use, disclosure or access to CPNI and required notification to customers to the extent personnel in the organization make sales referrals on inbound calls and for which the sales transaction is completed by other work groups. 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).
2. To the extent Credit and Collections and Global Fraud Management personnel market to customers on inbound calls, adequate training for the associated methods and procedures have been provided to such personnel to ensure an understanding of when they are and are not authorized to use CPNI as status of a customer's CPNI approval prior to use of CPNI for marketing purposes (47 C.F.R. §64.2009(a)(b)).

B. Training and Discipline

1. AT&T has established policies that explain the requirements for protecting CPNI. Employees in Asset Protection, Credit and Collections, and Global Fraud Management are required to adhere to the policies as well as the AT&T Code of Business Conduct. The Code of Business Conduct describes employees' obligation to protect customer information. There are also departmental standards and practices for ensuring compliance up to and including disciplinary actions against employees who do not adhere to CPNI rules.

C. CPNI Complaints and Breaches

Asset Protection personnel investigate CPNI security breach allegations, and Asset Protection has the responsibility for reporting all confirmed CPNI security breaches to law enforcement and customers as required.

1. AT&T Services, Inc. established M&Ps to manage reporting confirmed CPNI security breaches to the Federal Bureau of Investigation (FBI) and United States Secret Service (USSS). These M&Ps are periodically reviewed by Asset Protection personnel to ensure compliance. See 47 C.F.R. §64.2011 (a), (b) (1)-(3).

2. AT&T Services, Inc. established M&Ps for notifying customers of a confirmed CPNI security breach and the information is provided to the proper business unit for notifying customers. These M&Ps are reviewed with Asset Protection personnel periodically to ensure compliance. See 47 C.F.R. §64.2011 (c).

3. AT&T Services, Inc. developed M&Ps to ensure Asset Protection personnel maintain records of discovered breaches including, if available, dates of discovery and notification, a detailed description of the CPNI that was the breach subject, and the breach circumstances. These records are retained for a minimum of two (2) years. See 47 C.F.R. §64.2011 (d).

4. Methods and procedures are in place to support the requirements for tracking customer complaints regarding the unauthorized release of CPNI. The methods are reviewed semi-annually for completeness and communications are sent to all employees to increase awareness. Additionally, there is companywide training intended to help employees protect against social engineering that may lead to unauthorized release of CPNI. (§64.2009 (e), 64.2011).

D. Security and Authentication

1. For personnel in Credit and Collections and Global Fraud Management with access to CPNI, methods and procedures are in place to ensure adequate safeguards for the disclosure of CPNI. Procedures include specific authentication requirements prior to disclosing CPNI, including the use of passwords and back up authentication methods for lost or forgotten passwords as applicable. Additionally, procedures are in place to provide the required notifications for account changes as required by the rules (§64.2010 (a), (b), (c), (e) (f)).

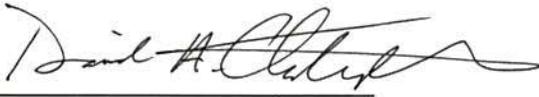
**AT&T Inc. CPNI Certification
Calendar Year 2013**

Date: 2/11/14

1. I, David Christopher, Chief Marketing Officer – AT&T Mobility (“Responsible Business Unit”) hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC’s rules, 47 C.F.R. § 64.2001 et. seq. (the “FCC’s CPNI rules”).

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: 

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF DAVID CHRISTOPHER, CHIEF MARKETING OFFICER – AT&T MOBILITY**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by the AT&T Mobility Marketing organization (“My Organization”) has adopted procedures that are intended to ensure compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC’s rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in My Organization, or (ii) developed by other organizations, in which case My Organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and correct potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals. To the extent applicable My Organization has:

1. Established and distributed methods and procedures (M&Ps) whereby personnel were not to disclose or permit access to customer’s CPNI for “out of category” services without customer approval or unless such disclosure or access was permitted under FCC rules and personnel were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer’s CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).
2. Established and distributed M&Ps whereby personnel were required to make a record of a customer’s consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).
3. Established and distributed M&Ps whereby personnel were prohibited from the use, disclosure or access to a customer’s individually identifiable CPNI, except where: (1) the customer granted “opt in approval” as defined in 47 C.F.R. §64.2003(k); (2) such use or

disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).

4. Established and distributed M&Ps whereby personnel were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby personnel were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).

5. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. 47 C.F.R. §64.2008(b) and (c).

6. Maintained an IVR and toll free number with voice mail whereby customers, at no additional cost, could avail themselves of an "opt-out" method. The IVR and voice mail were available 24 hours a day, seven days a week. See 47 C.F.R. §64.2008(d)(3)(v).

7. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).

8. Established M&Ps or implemented systems to clearly establish the status of a customer's CPNI approval prior to the use of CPNI. See 47 C.F.R. §64.2009(a).

B. Training and Discipline: My organization:

1. Requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, My Organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any

failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable My Organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication. To the extent applicable My Organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established methods and procedures prohibiting the disclosure of call detail over the phone unless the customer provides a password established in a manner consistent with 47 C.F.R. § 64.2010(e)
3. Established procedures for online access to CPNI in a manner consistent with 47 C.F.R. § 64.2010 (c) and (e).
4. Established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).

**AT&T Inc. CPNI Certification
Calendar Year 2013**

Date: February 14, 2014

1. I, Mel Coker, Chief Marketing Officer – Consumer Home Solutions (“Responsible Business Unit”) hereby certify, based upon my own personal knowledge, or based upon the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC’s rules, 47 C.F.R. § 64.2001 et. seq. (the “FCC’s CPNI rules”).

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature:



Mel Coker
Mel Coker

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF MEL COKER, CHIEF MARKETING OFFICER – CONSUMER HOME SOLUTIONS**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by Consumer Home Solutions (my organization) ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals. To the extent applicable my organization has:

1. Established and distributed methods and procedures (M&Ps) whereby personnel were not to disclose or permit access to customer's CPNI for "out of category" services without customer approval or unless such disclosure or access was permitted under FCC rules and personnel were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer's CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).
2. Established and distributed M&Ps whereby personnel were required to make a record of a customer's consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).

3. Established and distributed M&Ps whereby personnel were prohibited from the use, disclosure or access to a customer's individually identifiable CPNI, except where: (1) the customer granted "opt in approval" as defined in 47 C.F.R. §64.2003(k); (2) such use or disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).

4. Established and distributed M&Ps whereby personnel were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby personnel were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).

5. Maintained an IVR (toll free number) whereby customers, at no additional cost, could avail themselves of an "opt-out" method. The IVR and voice mail were available 24 hours a day, seven days a week. See 47 C.F.R. §64.2008(d)(3)(v).

6. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).

B. Training and Discipline: My organization:

1. Requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, my organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the

Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable my organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Sales and Marketing Campaigns. My Organization:

1. Maintains a record, for at least one year, of all approved marketing campaigns, including a description of the campaign, the type of CPNI used, and the products and services offered. See 47 C.F.R. § 64.2009(c).

2. Has established a supervisory review process for all outbound marketing campaigns to ensure all sales and marketing campaigns that propose to use CPNI are reviewed and approved. All proposed outbound marketing campaigns, requests for use of CPNI, and requests for marketing lists and customer data are submitted for review and require supervisory approval by the Database Marketing group. See 47 C.F.R. § 64.2009(d).

E. Security and Authentication. To the extent applicable:

1. Established processes and controls to notify the customer when a password, back-up means of authentication for lost or forgotten passwords, an online account, or an address of record is created or changed and to ensure that the content and delivery of such notice is in accordance with 47 C.F.R. § 64.2010(f). See also 47 C.F.R. § 64.2003(b). Specifically, My

Organization reacts to triggers from IT systems that notification must be sent. My Organization manages the content and delivery of such notifications and validates by reviewing customer counts, notification types, distribution method and distribution reports from internal and external vendors.

2. Established processes and controls to ensure that customer-initiated CPNI complaints or breaches, as "breach" is defined in 47 C.F.R. § 64.2011(e), are reported to AT&T Asset Protection for investigation and resolution and for complaint tracking and breach reporting purposes. See 47 C.F.R. § 64.2011. My Organization also, at the direction of various business units, manages the fulfillment of customer breach notifications by mail when such notifications are required.

3. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).

4. Established methods and procedures prohibiting the disclosure of call detail over the phone unless the customer is appropriately authenticated in a manner consistent with 47 C.F.R. § 64.2010(e)

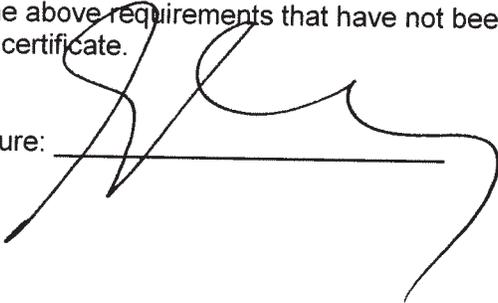
5. Established procedures for online access to CPNI in a manner consistent with 47 C.F.R. § 64.2010 (c) and (e).

AT&T Inc. CPNI Certification
Calendar Year 2013

Date: 2/10/14

1. I, José M. Gutiérrez, Executive Vice-President Wholesale Solutions hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.
2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").
3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: _____



**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF José M. Gutiérrez, Executive Vice-President Wholesale Solutions**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by the Wholesale Solutions and Access Management (my organization) ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules.

This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

- A. Customer CPNI Approvals.** To the extent applicable my organization has:
1. Established and distributed methods and procedures (M&Ps) whereby personnel were not to disclose or permit access to customer's CPNI for "out of category" services without customer approval or unless such disclosure or access was permitted under FCC rules and personnel were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer's CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).

2. Established and distributed M&Ps whereby personnel were required to make a record of a customer's consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).
3. Established and distributed M&Ps whereby personnel were prohibited from the use, disclosure or access to a customer's individually identifiable CPNI, except where: (1) the customer granted "opt in approval" as defined in 47 C.F.R. §64.2003(k); (2) such use or disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).
4. Established and distributed M&Ps whereby personnel were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby personnel were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).
5. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. 47 C.F.R. §64.2008(b) and (c).
6. Maintained an email method and toll free number with voice mail whereby customers, at no additional cost, could avail themselves of an "opt-out" method. The email method and voice mail were available 24 hours a day, seven days a week. See 47 C.F.R. §64.2008(d)(3).
7. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).
8. Established M&Ps or implemented systems to clearly establish the status of a customer's CPNI approval prior to the use of CPNI. See 47 C.F.R. §64.2009(a). Wholesale Solutions maintains a web-based CPNI database identifying the CPNI status

of all Wholesale Solutions customers. This database is updated in accordance with M&Ps designed to ensure the customer's status is continuously maintained.

B. Training and Discipline: My organization: Wholesale Solutions

1. Requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. The coursework developed in conjunction with the Wholesale Legal team is specific to the Wholesale Solutions organization. In addition, my organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable my organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication. To the extent applicable my organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established methods and procedures prohibiting the disclosure of call detail over the phone unless the customer provides a password established in a manner consistent with 47 C.F.R. § 64.2010(e)
3. Established procedures for online access to CPNI in a manner consistent with 47 C.F.R. § 64.2010 (c) and (e).
4. Established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).

AT&T Inc. CPNI Certification
Calendar Year 2013

Date: 2 | 4 | 14

1. I, William Hague, Executive Vice President - International, Alliances and Integration for AT&T Mobility and Consumer Markets ("Responsible Business Unit") hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: William W. Hague
William Hague, Executive Vice President - International, Alliances and Integration

EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013 OF WILLIAM HAGUE, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY AND CONSUMER MARKETS – INTERNATIONAL, ALLIANCES AND INTEGRATION

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC’s rules. This statement summarizes and explains the procedures and explains how these procedures were designed or adopted to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

My Organization is also responsible for the integration of the below listed six (6) wireless properties (“Properties”) that AT&T acquired in 2013 on the indicated date. For each Property, attached is a corresponding Schedule containing my explanation that summarizes and explains the procedures and explains how these procedures were designed or adopted to ensure the Property’s compliance with the CPNI rules during AT&T’s dates of ownership.

Schedule A: North State property, acquired on July 31, 2013

Schedule B: CORR property, acquired on September 9, 2013

Schedule C: Alltel property, acquired on September 20, 2013,

Schedule D: Comporium/HTC property, acquired on October 18, 2013

Schedule E: Element Wireless property, acquired on December 6, 2013

Schedule F: Long Lines property, acquired on December 20, 2013

A. Customer CPNI Approvals. To the extent applicable my organization has:

1. Established and distributed methods and procedures (M&Ps) whereby personnel were not to disclose or permit access to customer’s CPNI for “out of category” services without customer approval or unless such disclosure or access was permitted under FCC rules and personnel were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer’s CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).

2. Established and distributed M&Ps whereby personnel were required to make a record of a customer’s consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).

3. Established and distributed M&Ps whereby personnel were prohibited from the use, disclosure or access to a customer’s individually identifiable CPNI, except where: (1) the customer granted “opt in approval” as defined in 47 C.F.R. §64.2003(k); (2) such use or

disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).

4. Established and distributed M&Ps whereby personnel were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby personnel were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).

5. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. 47 C.F.R. §64.2008(b) and (c).

6. Maintained an IVR and toll free number with voice mail whereby customers, at no additional cost, could avail themselves of an "opt-out" method. The IVR and voice mail were available 24 hours a day, seven days a week. See 47 C.F.R. §64.2008(d)(3)(v).

7. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).

8. Established M&Ps or implemented systems to clearly establish the status of a customer's CPNI approval prior to the use of CPNI. See 47 C.F.R. §64.2009(a).

B. Training and Discipline: My organization:

1. Requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, my organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable my organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking

system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication. To the extent applicable my organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).

EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013 OF WILLIAM HAGUE, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY AND CONSUMER MARKETS – INTERNATIONAL, ALLIANCES AND INTEGRATION

Schedule A: North State Property

In accordance with Section 64.2009(e) of the CPNI rules, AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) has adopted procedures that are intended to ensure compliance of the North State Property, as defined below, with the FCC’s CPNI rules. This statement summarizes and explains the procedures and explains how these procedures were designed and adopted to ensure compliance with the CPNI rules.

On July 31, 2013, AT&T closed on its acquisition of certain wireless assets of North State Telephone Company’s (“Seller”). The acquisition included Seller’s North Carolina spectrum licenses, network assets, retail stores and approximately 27,000 wireless subscribers (the “North State Property”). During July 31, 2013, to December 31, 2013 (the “Time Period”), AT&T Mobility operated the North State Property under the North State brand. During the Time Period, AT&T received certain support services from Seller pursuant to a transition services agreement (“TSA”).

This Statement addresses AT&T’s operation of the North State Property during the Time Period. This Statement is based and relies on the following:

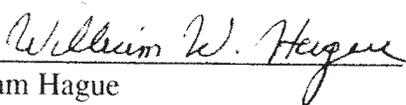
- (1) A CPNI Certification filed by Seller with the FCC on January 24, 2014 (“Seller Certification”) which states that during the calendar year 2013, Seller established operating procedures that are adequate to ensure the North State Property’s compliance with the requirements of the FCC’s CPNI rules (“Legacy Sales Practices”).
- (2) A Subcertification dated January 22, 2014, from Seller to AT&T stating that during the Time Period, Seller continued the Legacy Sales Practices in its provision of services to AT&T under the TSA.

A. Customer CPNI Approvals. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

B. Training and Discipline. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

C. CPNI Complaints and Breaches. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

D. Security and Authentication. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

Date: 
William Hague



Clint Farabow
Senior Analyst
External Affairs

By Electronic Filing

January 24, 2014

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

RE: CPNI Certification

EB Docket 06-36

Dear Ms. Dortch:

Attached to this letter is the Annual 47 C.F.R. § 64.2009(e) CPNI Certification and statement of procedures for operational compliance for North State Telephone Company, North State Communications Long Distance, LLC and North State Communications Advanced Services LLC, all of which are d/b/a North State Communications.

This filing was completed via the FCC's Electronic Filing System with a copy e-mailed to Best Copy and Printing. (fcc@bcpiweb.com)

Sincerely,

A handwritten signature in black ink that reads "Clint Farabow". The signature is written in a cursive, flowing style.

Clint Farabow

NORTH STATE COMMUNICATIONS

P. O. Box 2326, High Point, NC 27261 336-886-3600

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2013 covering the prior calendar year 2013

Date signed: January 22, 2014

Names of Companies Covered by this Certification:

499 Filer ID

North State Telephone Company d/b/a North State Communications	806706
North State Communications Long Distance, LLC, d/b/a North State Communications	803194
North State Communications Advanced Services, LLC, d/b/a North State Communications	827546
North State Communications LLC, d/b/a North State Communications	828662

Name of signatory: Lynn Welborn

Title of signatory: Vice President, Corporate Administration

I, Lynn Welborn, certify that I am an officer of the affiliated companies named above (collectively and individually "Company"), 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 CPNI rules of the Federal Communications Commission ("Commission"). *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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The Company 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 2013 or related to 2013. The Company is not aware of any attempts by pretexters to access the CPNI of Company customers and thus has not had to take any actions against data brokers. The Company has taken steps to protect CPNI from unauthorized access and has described these steps in the accompanying statement.

The Company has not received any 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: Lynn B. Welborn Date: January 22, 2014

Attachment

NORTH STATE COMMUNICATIONS
P. O. Box 2326, High Point, NC 27261 336-886-3600

<u>Names of Companies Covered by Statement</u>	<u>499 Filer ID</u>
North State Telephone Company, d/b/a North State Communications	806706
North State Communications Long Distance, LLC, d/b/a North State Communications	803194
North State Communications Advanced Services, LLC, d/b/a North State Communications	827546
North State Communications LLC, d/b/a North State Communications	828662

2012 ANNUAL STATEMENT OF FCC CPNI RULE COMPLIANCE
(EB Docket No. 06-36)
January 10, 2014

This statement serves to explain how the North State Communications telecommunication carrier affiliates named above (collectively and individually "Company"), are complying with Federal Communications Commission ("FCC") rules related to the privacy of customer information. The type of information for which customer privacy is protected by the FCC's rules is called "customer proprietary network information" ("CPNI"). The FCC's rules restricting telecommunication company use of CPNI are contained at Part 64, Subpart U of the FCC's rules (47 C.F.R. §§ 64.2000-2011).

All subsequent references to rule Sections refer to rules under Part 64, Subpart U unless indicated otherwise.

1. Identification of CPNI

The Company has established procedures and trained employees having access to, or occasion to use customer data, to identify what customer information is CPNI consistent with the definition of CPNI under the Section 64.2003(g) and Section 222(f)(1) of the Communications Act of 1934 as amended (47 U.S.C. § 222(f)(1)).

2. Identification of Services Affected by CPNI Rules

The Company has established procedures and trained employees to recognize the different types of telecommunications and non-telecommunications services that affect how the Company uses CPNI.

3. Identification of Permissible Uses of CPNI without Customer Authorization

The Company has established procedures and trained employees having access to, or occasion to use CPNI, to identify uses of CPNI not requiring customer authorization under Section 64.2005.

4. Identification of Uses of CPNI Requiring Customer Authorization

The Company has established procedures and trained employees having access to, or occasion to use CPNI, to identify uses of CPNI requiring customer authorization under Section 64.2007.

5. Customer Notification and Authorization Process

The Company has established procedures, and trained employees responsible for obtaining customer authorization to use CPNI for marketing purposes, regarding the notice and approval

January 22, 2014

Delivered via Email to GK764P@att.com

Ms. Georgia Kruse
Director – Project Management
International, Alliances & Integrations
AT&T Mobility Services LLC

RE: Sub-Certification for CPNI Reporting Year 2013

Dear Ms. Kruse:

I, Lynn Welborn, certify that I am an officer of North State Telephone Company (“Company”), 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 CPNI rules of the Federal Communications Commission (“Commission”). *See* 47 C.F.R. § 64.2001 *et seq.*

On July 31, 2013, FCC radio licenses and assets held by Company were acquired by a subsidiary of AT&T pursuant to FCC authorizations. Company continues to operate the network and offer wireless devices pursuant to the terms of a transition services agreement (“TSA”) with the AT&T subsidiary. This Certification covers the portion of calendar year 2013 following the above-referenced transaction, during which AT&T owned the assets and Company operated pursuant to the TSA. This period of time included July 31, 2013 through December 31, 2013. During this period of time, Company continued to ensure CPNI compliance and execute CPNI operating procedures.

Attached to this certification is an accompanying statement explaining how the Company’s procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission’s rules.

The Company 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 2013 or related to 2013. The Company is not aware of any attempts by pretexters to access the CPNI of Company customers and thus has not had to take any actions against data brokers. The Company has taken steps to protect CPNI from unauthorized access and has described these steps in the accompanying statement.

The Company has not received any 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: Lynn B. Welborn Date: January 22, 2014

Attachment

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013 OF WILLIAM
HAGUE, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY AND CONSUMER
MARKETS – INTERNATIONAL, ALLIANCES AND INTEGRATION**

Schedule B: Corr Property

In accordance with Section 64.2009(e) of the CPNI rules, AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) has adopted procedures that are intended to ensure compliance of the Corr Property, as defined below, with the FCC’s CPNI rules. This statement summarizes and explains the procedures and explains how these procedures were designed and adopted to ensure compliance with the CPNI rules.

On September 9, 2013, AT&T closed on its acquisition of certain wireless assets of Corr Wireless Communications, LLC (“Seller”). The acquisition included Seller’s Alabama wireless spectrum licenses, network assets, retail stores and approximately 21,000 wireless subscribers (the “Corr Property”). During September 9, 2013, to December 31, 2013 (the “Time Period”), AT&T Mobility operated the Corr Property under the Corr Wireless brand. During the Time Period, AT&T received certain support services from Seller pursuant to a transition services agreement (“TSA”).

This Statement addresses AT&T’s operation of the Corr Property during the Time Period. This Statement is based and relies on the following:

- (1) A CPNI Certification filed by Seller with the FCC on February 3, 2014 (“Seller Certification”) which states that during its operation of the Corr Property from January 1, 2013 to September 8, 2013, Seller established operating procedures that are adequate to ensure the Corr Property’s compliance with the requirements of the FCC’s CPNI rules (“Legacy Sales Practices”).
- (2) A CPNI Certification dated January 21, 2014, by Seller which states that during the Time Period, Seller continued the Legacy Sales Practices in its provision of services to AT&T under the TSA.

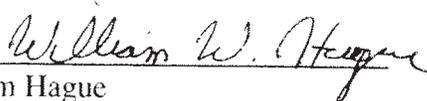
A. Customer CPNI Approvals. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

B. Training and Discipline. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

C. CPNI Complaints and Breaches: During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

D. Security and Authentication. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

Date:



William Hague

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

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification covering calendar year 2013,
namely January 1, 2013 through September 9, 2013

Date filed:

Name of company covered by this certification:

Corr Wireless Communications, LLC

Form 499 Filer ID 801004

Address: P.O. Box 1500
600 Third Avenue East
Oneonta, Alabama 35121

Name of signing officer: Kevin Hankins

Title of signatory: Chief Operating Officer of Managing Member

CERTIFICATION

I, Kevin Hankins, hereby 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 Customer Proprietary Network Information (CPNI) rules set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the rules of the Federal Communications Commission.

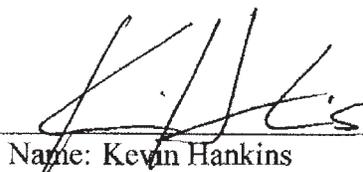
This Certification covers the portion of calendar year 2013 during which Corr Wireless Communications LLC ensured CPNI compliance and executed CPNI operating procedures. This period of time included January 1, 2013 through September 8, 2013, and is hereinafter referred to as the "reporting period of 2013."

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 reporting period of the past year.

The company has not received customer complaints in the reporting period of 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.



Name: Kevin Hankins

Title: Chief Operating Officer of Managing Member,
Cellular South, Inc.

Date: 1-21-14

Attachment: Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers (if applicable)
Summary of customer complaints (if applicable)

Company Names (referred to as "Carrier"):

Corr Wireless Communications, LLC

STATEMENT

Carrier has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Carrier has adopted a manual and keeps it updated with FCC CPNI rule revisions, and has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier continually educates and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.
- Carrier has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
- Carrier maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes 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.
- Carrier has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. Specifically, Carrier's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.
- Carrier has implemented procedures to properly authenticate customers prior to disclosing CPNI over the telephone, at Carrier's retail locations or otherwise. In connection with these procedures, Carrier has established a system of passwords and back-up authentication methods which complies with the requirements of applicable Commission rules.
- Carrier has established procedures to ensure that customers will be immediately notified of account changes including changes to passwords, back-up means of authentication for lost or forgotten passwords, or address of record.

- Carrier has established procedures to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with FCC timelines.
- Carrier took the following actions against data brokers in the reporting period of 2013, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission: No action taken
- The following is information Carrier has with respect to the processes pretexters are using to attempt to access CPNI, and [if any] what steps carriers are taking to protect CPNI: No information received
- The following is a summary of all customer complaints received in the reporting period of 2013 regarding the unauthorized release of CPNI:
 - Number of customer complaints Carrier received in the reporting period of 2013 related to unauthorized access to CPNI, or unauthorized disclosure of CPNI: _____ 0 _____
 - Category of complaint:
 - ___ Number of instances of improper access by employees
 - ___ Number of instances of improper disclosure to individuals not authorized to receive the information
 - ___ Number of instances of improper access to online information by individuals not authorized to view the information
 - ___ Number of other instances of improper access or disclosure
 - Summary of customer complaints received in the reporting period of 2013 concerning the unauthorized release of CPNI: _____

The compliant practices described herein were conducted during the reporting period of 2013.

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

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification covering calendar year 2013,
namely September 9, 2013 through December 31, 2013

Date filed:

Name of company covered by this certification:

Corr Wireless Communications, LLC

Form 499 Filer ID 801004

Address: P.O. Box 1500
600 Third East Avenue
Oneonta, Alabama 35121

Name of signing officer: Kevin Hankins

Title of signatory: Chief Operating Officer of Managing Member

CERTIFICATION

I, Kevin Hankins, hereby 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 Customer Proprietary Network Information (CPNI) rules set forth in 47 C.F.R. §§ 64.2001 *et seq.* of the rules of the Federal Communications Commission.

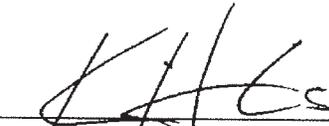
On September 9, 2013 FCC radio licenses and assets held by Corr Wireless Communications LLC were acquired by a subsidiary of AT&T pursuant to FCC authorizations. Corr Wireless continues to operate the network and offer wireless devices pursuant to terms of a transition services agreement (TSA) with the AT&T subsidiary. This Certification covers the portion of calendar year 2013 following the transaction, during which AT&T owned the assets and Corr Wireless Communications LLC operated pursuant to the TSA, continuing to ensure CPNI compliance and execute CPNI operating procedures. This period of time included September 9, 2013 through December 31, 2013, and is hereinafter referred to as the "reporting period of 2013."

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 reporting period of the past year.

The company has not received customer complaints in the reporting period of 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.



Name: Kevin Hankins

Title: Chief Operating Officer of Managing Member,
Cellular South, Inc.

Date: 1-21-14

Attachment: Accompanying Statement explaining CPNI procedures
Explanation of actions taken against data brokers (if applicable)
Summary of customer complaints (if applicable)

Company Names (referred to as "Carrier"):

Corr Wireless Communications, LLC

STATEMENT

Carrier has established operating procedures that ensure compliance with the Federal Communication Commission ("Commission") regulations regarding the protection of customer proprietary network information ("CPNI").

- Carrier has adopted a manual and keeps it updated with FCC CPNI rule revisions, and has designated a CPNI compliance officer to oversee CPNI training and implementation.
- Carrier continually educates and trains its employees regarding the appropriate use of CPNI. Carrier has established disciplinary procedures should an employee violate the CPNI procedures established by Carrier.
- Carrier has implemented a system whereby the status of a customer's CPNI approval can be determined prior to the use of CPNI.
- Carrier maintains a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI. Carrier also maintains a record of any and all instances where CPNI was disclosed or provided to third parties, or where third parties were allowed access to CPNI. The record includes 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.
- Carrier has established a supervisory review process regarding compliance with the CPNI rules with respect to outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. Specifically, Carrier's sales personnel obtain supervisory approval of any proposed outbound marketing request for customer approval regarding its CPNI, and a process ensures that opt-out elections are recorded and followed.
- Carrier has implemented procedures to properly authenticate customers prior to disclosing CPNI over the telephone, at Carrier's retail locations or otherwise. In connection with these procedures, Carrier has established a system of passwords and back-up authentication methods which complies with the requirements of applicable Commission rules.
- Carrier has established procedures to ensure that customers will be immediately notified of account changes including changes to passwords, back-up means of authentication for lost or forgotten passwords, or address of record.

- Carrier has established procedures to notify law enforcement and customer(s) of unauthorized disclosure of CPNI in accordance with FCC timelines.
- Carrier took the following actions against data brokers in the reporting period of 2013, including proceedings instituted or petitions filed by Carrier at a state commission, in the court system, or at the Federal Communications Commission: No action taken
- The following is information Carrier has with respect to the processes pretexters are using to attempt to access CPNI, and [if any] what steps carriers are taking to protect CPNI: No information received
- The following is a summary of all customer complaints received in the reporting period of 2013 regarding the unauthorized release of CPNI:
 - Number of customer complaints Carrier received in the reporting period of 2013 related to unauthorized access to CPNI, or unauthorized disclosure of CPNI: _____ 0 _____
 - Category of complaint:
 - ___ Number of instances of improper access by employees
 - ___ Number of instances of improper disclosure to individuals not authorized to receive the information
 - ___ Number of instances of improper access to online information by individuals not authorized to view the information
 - ___ Number of other instances of improper access or disclosure
 - Summary of customer complaints received in the reporting period of 2013 concerning the unauthorized release of CPNI: _____

The compliant practices described herein were conducted during the reporting period of 2013.

EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013 OF WILLIAM HAGUE, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY AND CONSUMER MARKETS – INTERNATIONAL, ALLIANCES AND INTEGRATION

Schedule C: Alltel Property

In accordance with Section 64.2009(e) of the CPNI rules, AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) has adopted procedures that are intended to ensure compliance with the FCC’s CPNI rules for certain wireless properties acquired by AT&T Mobility during 2013. This statement summarizes and explains the procedures and explains how these procedures were designed and adopted to ensure compliance with the CPNI rules.

On September 20, 2013, AT&T closed its acquisition of Atlantic Tele-Network, Inc.’s (“Seller’s”) U.S. retail wireless operations, operated under the Alltel brand (the “Alltel Property”). The acquisition included wireless properties in six states, including licenses, CDMA network assets, retail stores and approximately 585,000 wireless subscribers across six (6) states: North Carolina, South Carolina, Illinois, Idaho, Ohio and Georgia.

During September 20 to December 31, 2013 (the “Time Period”), AT&T operated the Alltel Property as a “stand alone” market continuing to sell and provide CDMA service under the Alltel brand to existing and prospective customers. The Alltel Property’s operations are run by AT&T employees most of whom are acquired Alltel employees. During the Time Period, AT&T has worked on deploying its GSM technology over the acquired CDMA networks and plans on migrating Alltel customers to AT&T’s systems in 2014 after the deployment is complete.

This Statement addresses AT&T’s operation of the Alltel Property during the Time Period. This Statement is based and relies on the following:

1. A CPNI Certification filed by Seller on February 10, 2014 with the FCC (“Seller Certification”) which states that during its operation of the Alltel Property from January 1 to September 20, 2013, Seller established safeguards and operating procedures (“Legacy Sales Practices”) adequate to ensure the Alltel Property’s compliance with the requirements of the CPNI rules.
2. A CPNI Certification dated February 10, 2014, by Lesa Handly, Integration Lead - International, Alliances and Integration for AT&T Mobility and Consumer Markets, and Chief Operating Officer of the Alltel Property during the Time Period. Ms. Handly’s Certification states that during the Time Period, AT&T followed the Legacy Sales Practices in its operation of the Alltel Property.

For the AT&T employees covered by this Schedule C, the described processes and procedures have either been (i) developed and implemented in My Organization, or (ii) developed by Seller or other organizations, in which case My Organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating

procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals.

During the Time Period, My Organization followed the Legacy Sales Practices memorialized in the Seller Certification wherein Seller states that said Legacy Sales Practices methods and procedures were in compliance with the Commission's CPNI rules.

B. Training and Discipline:

1. My Organization required all employees to review AT&T's Code of Business conduct which includes general information regarding protection of customer records and system access policies. In addition, CPNI specific training was conducted for 444 former Alltel employees identified by Corporate Compliance. New employees are required to complete this training within thirty (30) days of their start date. AT&T maintains a record of completion of review of the Code of Business conduct. AT&T further required all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. See 47 C.F.R. §64.2009 (b).

2. My Organization maintained a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches:

During the Time Period, My Organization followed the Legacy Sales Practices memorialized in the Seller Certification wherein Seller states that said Legacy Sales Practices methods and procedures were in compliance with the Commission's CPNI rules.

D. Security and Authentication.

During the Time Period, My Organization followed the Legacy Sales Practices memorialized in the Seller Certification wherein Seller states that said Legacy Sales Practices methods and procedures were in compliance with the Commission's CPNI rules.

Date:

William W. Hague
William Hague

1001 Technology Drive
Little Rock, AR 72223

www.awcc.com



February 10, 2014

VIA ECFS

Ms. Darlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, Suite TW-245
Washington D.C. 20554

Re: Annual 64.2009(e) CPNI Certification for 2013; EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e) of the Commission's Rules, Allied Wireless Communications Corporation hereby files its annual certification of compliance with the Commission's customer proprietary network information rules for the period January 1, 2013 through September 20, 2013.

Please contact the undersigned at 501-448-1249 should you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'Rohan Ranaraja', is written over a faint, light-colored signature line.

Rohan Ranaraja

Attachments:

ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION

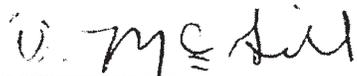
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for Allied Wireless Communications Corporation

1. Date filed: February 10, 2014
2. Name of company covered by this certification: Allied Wireless Communications Corporation (see attachment)
3. Form 499 Filer ID: 828499 (see attachment)
4. Name and title of signatory: Wade McGill, Chief Administrative Officer
5. Period covered by this certification: January 1, 2013 through September 20, 2013 (“Relevant Period”)
6. Certification:

I, Wade McGill, 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, as described in Sections A through J of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION (“Statement”), 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 set forth in section 64.2001 et seq. of the Commission’s rules, including an explanation of actions taken against data brokers and a summary of customer complaints received during the Relevant Period covering the unauthorized release of CPNI.



Wade McGill

Chief Administrative Officer

Attachments: Companies covered by Annual CPNI Certification
Statement of Operating Procedures

**COMPANIES COVERED BY ANNUAL CPNI CERTIFICATION OF ALLIED
WIRELESS COMMUNICATIONS CORPORATION**

Allied Wireless Communications Corporation (828499)
Georgia RSA #8 Limited Partnership (806211)

**STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R.
SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK
INFORMATION FOR THE PERIOD JANUARY 1, 2013 TO SEPTEMBER 20, 2013**

The following statement submitted on behalf of Allied explains how the operating procedures of Allied ensured that it was in compliance with the Commission's CPNI rules, as referenced herein and set forth in 47 C.F.R. Subpart U.

A. CPNI Use and Customer Approval

In accordance with 47 CFR 64.2005(a), Allied used CPNI internally for the purpose of providing a customer with the requested service and for marketing service offerings within the categories of service to which the customer subscribed from Allied. During the Relevant Period, Allied offered CMRS and information services. Consistent with 47 CFR 64.2005(b), Allied did not use, disclose, or permit access to CPNI to market telecommunications service offerings outside the category of service to which the customer subscribed. Allied used CPNI derived from the provision of CMRS for the provision of CPE and information services. Allied did not solicit customer consent to use CPNI in a manner that was beyond its then existing service relationship and Allied did not consider its customer to have granted approval for such CPNI use. As a result, the requirements contained in the revised section 64.2007(b) (Use of Opt-Out and Opt-In Approval Processes) pertaining to the approval process applicable to using customer's individually identifiable CPNI for marketing communications-related services to such customers did not apply to Allied's operational use of CPNI during the Relevant Period.

B. Sales and Marketing Campaigns

Pursuant to 47 CFR 64.2009, Allied reviewed sales and marketing campaigns that used CPNI. All such campaigns were conducted to market services within the category of service to which the customer subscribed from Allied in accordance with 47 CFR 64.2005(a). Allied did not engage in cross service marketing campaigns. In addition and consistent with 47 CFR 64.2009(d), Allied had a supervisory review process to evaluate the proposed use of CPNI in outbound marketing campaigns. Allied restricted the ability to create marketing campaigns in order to ensure compliance with the CPNI rules. The persons with authority to approve campaigns which used CPNI were previously authorized employees.

Consistent with 47 CFR 64.2009(c), Allied maintained records of the campaigns which used CPNI that were conducted by authorized personnel. These records contain a description of each campaign, the specific CPNI that was used in the campaign, and the products and services that were offered as a part of the campaign. This information is retained for at least one year.

C. Training and Disciplinary Process

Allied personnel and agents were trained as to when they were and were not authorized to use CPNI and Allied's Customer Privacy Policy expressly established a disciplinary process applicable to employees and agents in the event it was determined that such policy had been violated. A violation of the policy and failure to protect customer information may lead to disciplinary action, up to and including termination.

D. Security Governance

Allied maintained policies, procedures, internal controls and systems designed to protect all of the data collected, generated, created, stored, managed, transmitted or otherwise handled by Allied employees.

E. Billing Records, Network Records, and Information

Allied maintained billing detail data, call detail data, and network record data in applications secured by networks, systems, policies and processes designed to control, monitor, and limit access to authorized users with legitimate business needs. Allied's corporate security team reviewed new applications and enhancements for compliance with existing security practices, which included requirements for access and authentication controls.

F. Data Centers

All data centers had processes and procedures in place for controlling physical access into the data centers along with controlling system access. Compliance with security policies was reviewed by Allied's Information Technology Security Manager during the Relevant Period for its systems.

G. Safeguards on the Disclosure of CPNI

(1) Safeguarding CPNI

Allied's account verification policy established the circumstances and limitations under which Allied call center and retail employees were allowed to disclose CPNI. These employees were monitored for compliance with Allied's account verification procedures.

Allied employees were trained to keep sensitive customer data strictly confidential and suspected breaches of customer confidentiality were investigated by corporate security teams. In addition to investigating reported incidents, security teams periodically conducted reviews of various systems to identify potential unauthorized access to customer data. Allied required newly-hired employees to sign an "Employee Agreement on Non-Disclosure and Non-Solicitation," which prohibited employees from disclosing information that was confidential to any third party. Confirmed unauthorized disclosures of customer information were subject to discipline, up to and including termination and referrals to law enforcement authorities where

deemed appropriate. Policies, practices, and technologies were used to limit employee access to customer records on a business need basis.

Allied's privacy statement described how Allied used, maintained and protected customer information, including CPNI. During the Relevant Period, this statement was available to all customers at www.alltelwireless.com by clicking on "Privacy Statement" at the bottom of Allied's home page. In addition, Allied's contracts with independent contractors that had access to confidential customer data were required to contain safeguards necessary to protect that data.

(2) Telephone Access to CPNI

By policy, reinforced with training and monitoring, Allied customer service representatives were prohibited from disclosing call detail (as defined in 47 CFR 64.2003(d)) over the telephone unless the customer service representative called the customer at the telephone number of record (as defined in 47 CFR 64.2003(q)). A customer service representative was allowed to assist the customer in the event an authenticated customer first identified the call to the representative without assistance during a call initiated by the customer. Upon request, Allied would mail a copy of the call details to the customer's address of record. In the event a customer's address of record had changed in the thirty days prior to the telephone request, Allied did not mail the required call detail. Instead, such customer is allowed to utilize online or in-store access. Allied's policy did not permit faxing of call detail.

(3) Online Access to CPNI

Allied maintained an online account retrieval system called "My Account" whereby Allied customers could register their account and subsequently login to access their account information and CPNI only after providing a valid password. During the Relevant Period, Allied's operating procedures were adequate to ensure compliance with the CPNI rules related to online access to CPNI, including a requirement that all wireless phone customers who register for My Account receive a text message to the designated handset on the account being registered. Pursuant to these procedures, a code in the text message would be required to complete the registration process.

Allied customers who wanted online access to their account information and CPNI first needed to register their account on My Account. Prior to beginning the registration process, customers were required to provide Allied their mobile number. The registration process required customers to: (1) provide their name; (2) create a unique user identification; (3) create a password; and (4) provide their electronic mail address. Wireless phone customers were sent a text message containing a unique code to their handset which was then used to complete the My Account registration process. Thereafter customers were required to utilize their user identification and password for online access to CPNI.

Additionally, Allied provided all customers the ability to block online access to their account and CPNI.

(4) Establishment of a Password and Back-Up Authentication Methods for Lost of Forgotten Passwords

Allied made available a backup authentication method for wireless phone customers who had forgotten their My Account password. This backup authentication method did not prompt the customer for readily identifiable biographical or account information. If the wireless phone customer did not provide the correct response for the backup authentication method, the customer was sent a code via text message to their handset. The customer was required to provide this code to Allied prior to establishing a new password.

(5) Notification of Account Changes

Allied immediately notified customers via text message to their handset or United States mail to their address of record, when a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record was created or changed. Allied did not reveal the changed information.

(6) In-Store Access to CPNI

Allied required customers to present valid photo identification and verified that identity matched the account information prior to disclosing CPNI at an Allied retail location and at Allied agent retail locations.

H. Notification of CPNI Security Breaches

Allied's existing processes ensured compliance with the CPNI rules. In the event of a confirmed CPNI breach, Allied has established procedures to notify customers in accordance with the CPNI breach notification rules.

I. Summary of Customer Complaints Regarding the Unauthorized Release of CPNI

During the Relevant Period, Allied did not receive customer complaints concerning the unauthorized release of CPNI.

J. Action Taken Against Data Brokers

During the Relevant Period, Allied did not initiate any action against data brokers.

AT&T Inc. CPNI Certification
September 20, 2013 to December 31, 2013

Date: February 10, 2014

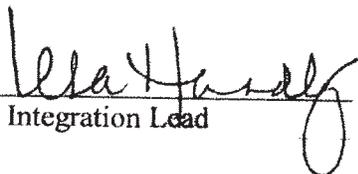
1. I, Lesa Handly, Integration Lead - International, Alliances and Integration for AT&T Mobility and Consumer Markets ("Responsible Business Unit") hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: _____

Lesla Handly, Integration Lead

A handwritten signature in black ink, appearing to read "Lesla Handly", written over a horizontal line. The signature is cursive and somewhat stylized.

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR SEPTEMBER 20 TO
DECEMBER 31, 2013, OF LESA HANDLY, AT&T INTEGRATION LEAD, AT&T
MOBILITY AND CONSUMER MARKETS – INTERNATIONAL, ALLIANCES AND
INTEGRATION**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) ensures the compliance of the Alltel Property, as defined below, with the specific requirements set forth in Subpart U- Customer Proprietary Network Information of the FCC’s rules. This statement summarizes and explains the procedures and explains how these procedures were designed or adopted from the Seller, as defined below, to ensure compliance with the CPNI rules.

On September 20, 2013, AT&T closed its acquisition of Atlantic Tele-Network, Inc.’s (“Seller’s”) U.S. retail wireless operations, operated under the Alltel brand. The acquisition included wireless properties in six states, including licenses, CDMA network assets, retail stores and approximately 585,000 wireless subscribers across six (6) states: North Carolina, South Carolina, Illinois, Idaho, Ohio and Georgia (the “Alltel Property”).

During September 20 to December 31, 2013 (the “Time Period”), AT&T operated the Alltel Property as a “stand alone” market continuing to sell and provide CDMA service under the Alltel brand to existing and prospective customers. The Alltel Property’s operations are run by AT&T employees most of whom are acquired Alltel employees. During the Time Period, AT&T worked on deploying its GSM technology over the acquired CDMA networks and plans on migrating Alltel customers to AT&T’s systems in 2014 after the deployment is complete.

My Statement addresses AT&T’s operation of the Alltel Property during the Time Period. My Statement is based and relies, in part, on the CPNI Certification filed by Sellers on February 10, 2014 which states that during its operation of the Alltel Property from January 1 to September 20, 2013, Seller established safeguards and operating procedures (“Legacy Sales Practices”) adequate to ensure the Alltel Property’s compliance with the requirements of the FCC’s CPNI rules. In addition, I served as the Integration Lead of the Alltel Property during the Time Period and I oversaw the Alltel Property’s continued use of the Legacy Sales Practices.

For the AT&T employees covered by my Certification, the described processes and procedures have either been (i) developed and implemented in My Organization, or (ii) developed by other organizations, in which case My Organization operates in compliance with such applicable processes and procedures. The Alltel Property has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent the Alltel Property discovers or is made aware of an error, the Alltel Property investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals.

1. AT&T acquired wireless properties, including licenses, network assets, employees and approximately 585,000 subscribers from Sellers. During the Time Period, AT&T followed the Legacy Sales Practices. Sellers filed a certification with the Commission on February 10, 2014,

wherein they stated that such sales methods and procedures were in compliance with the Commission's CPNI rules.

2. The Alltel Property used CPNI internally for the purpose of providing a customer with the requested service and for marketing service offerings within the categories of service to which the customer subscribed from Alltel. During the Time Period, Alltel offered CMRS and information services. Consistent with 47 CFR 64.2005(b), the Alltel Property did not use, disclose, or permit access to CPNI to market telecommunications service offerings outside the category of service to which the customer subscribed.

3. The Alltel Property used CPNI derived from the provision of CMRS for the provision of CPE and information services.

4. The Alltel Property did not solicit customer consent to use CPNI in a manner that was beyond its then existing service relationship and it did not consider its customer to have granted approval for such CPNI use. As a result, the requirements contained in the revised section 64.2007(b) (Use of Opt-Out and Opt-In Approval Processes) pertaining to the approval process applicable to using customer's individually identifiable CPNI for marketing communications-related services to such customers did not apply to the Alltel Property's operational use of CPNI during the Time Period.

B. Training and Discipline:

1. The Alltel Property requires all personnel to complete specific CPNI training annually. Training includes review of the Customer Privacy Policy and all corporate employees are also required to review the CPNI Policy. See 47 C.F.R. §64.2009 (b). In addition, after the acquisition of the Alltel Property, AT&T conducted additional CPNI training for 444 former Alltel employees identified by Corporate Compliance.

2. The Alltel Property maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: Legacy Sales Practices ensured compliance with the CPNI rules. In the event of a confirmed CPNI breach, the Alltel Property established procedures to notify customers in accordance with the CPNI breach notification rules. In addition, relevant personnel were apprised that they are required to take certain steps, including notifying the appropriate person, if they suspect or determine there has been a breach of CPNI or if they receive any customer complaint regarding unauthorized access to, disclosure or release of CPNI. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication.

1. During the Time Period, the Alltel Property followed the Legacy Sales Practices. Sellers filed a certification with the Commission on February 10, 2014, wherein they stated that such sales methods and procedures were in compliance with the Commission's CPNI rules.

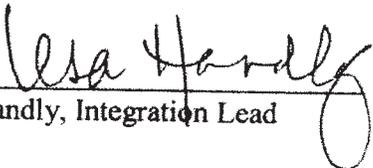
2. The Alltel Property established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).

3. The Alltel Property established methods and procedures prohibiting the disclosure of call detail over the phone unless the customer provides a password established in a manner consistent with 47 C.F.R. § 64.2010(e) or the customer service representative calls the customer at the telephone number of record pursuant to 47 C.F.R. § 64.2010(b).

4. The Alltel Property established procedures for online access to CPNI in a manner consistent with 47 C.F.R. § 64.2010 (c) and (e).

4. The Alltel Property established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).

Date:



Lesa Handly, Integration Lead

EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013 OF WILLIAM HAGUE, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY AND CONSUMER MARKETS – INTERNATIONAL, ALLIANCES AND INTEGRATION

Schedule D:HTC/Comporium Property

In accordance with Section 64.2009(e) of the CPNI rules, AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) has adopted procedures that are intended to ensure compliance of the Property, as defined below, with the FCC’s CPNI rules. This statement summarizes and explains the procedures and explains how these procedures were designed and adopted to ensure compliance with the CPNI rules.

On October 18, 2013, AT&T closed on an agreement with Horry Telephone Cooperative, Inc. (“HTC”) and Comporium Wireless, LLC (“CW”) to create a limited liability company managed (“LLC”) and controlled by AT&T Mobility to provide wireless services in several non-contiguous counties (or partial counties) in South Carolina (the “Property”). HTC and CW (“Sellers”) contributed licenses, subscribers and network equipment and ATT Mobility contributed subscribers and licenses in exchange for equity interests in the LLC. During October 18, 2013, to December 31, 2013 (the “Time Period”), Sellers continued to operate the Property and sell their wireless services under the Sellers’ brand. During the Time Period, AT&T received certain support services from Sellers pursuant to a transition services agreement (“TSA”).

This Statement addresses AT&T’s operation of the Property during the Time Period. This Statement is based and relies on the following:

- (1) A CPNI Certification filed by CWS with the FCC on February 3, 2014 (“CW Certification”) which states that during its operation of the Property from January 1, 2013, to October 17, 2013, CW established operating procedures that are adequate to ensure the Property’s compliance with the requirements of the CPNI rules (“CW Legacy Sales Practices”).
- (2) A CPNI Sub-Certification dated February 3, 2014, from CW to AT&T Mobility Services LLC which states that during the Time Period, CW continued the CW Legacy Sales Practices in its provision of services to AT&T under the TSA.
- (3) A CPNI Certification filed by HTC with the FCC on February 3, 2014 (“HTC Certification”) which states that during its operation of the Property from January 1, 2013, to October 17, 2013, HTC established operating procedures that are adequate to ensure the Property’s compliance with the requirements of the CPNI rules (“HTC Legacy Sales Practices”).
- (4) A CPNI Sub-Certification dated January 14, 2014, from HTC to AT&T Mobility Services LLC which states that during the Time Period, HTC continued the HTC Legacy Sales Practices in its provision of services to AT&T under the TSA.

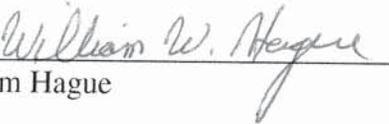
A. Customer CPNI Approvals. During the Time Period, Sellers under the TSA continued to follow their respective Legacy Sales Practices memorialized in the CW Certification and HTC Certification.

B. Training and Discipline. During the Time Period, Sellers under the TSA continued to follow their respective Legacy Sales Practices memorialized in the CW Certification and HTC Certification.

C. CPNI Complaints and Breaches: During the Time Period, Sellers under the TSA continued to follow their respective Legacy Sales Practices memorialized in the CW Certification and HTC Certification.

D. Security and Authentication. During the Time Period, Sellers under the TSA continued to follow their respective Legacy Sales Practices memorialized in the CW Certification and HTC Certification.

Date:



William Hague

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2014 covering the prior calendar year 2013

1. Date filed: **02/03/2014**
2. Name of company(s) covered by this certification: **Comporium, Inc., Fort Mill Telephone Company (d/b/a "Comporium Communications"), Lancaster Telephone Company (d/b/a "Comporium Communications"), Citizens Telephone Company (d/b/a "Comporium Communications"), Community Long Distance, Inc (d/b/a "Comporium Communications"), and Springboard Telecom, LLC.**

This certification covers Comporium Wireless, LLC, for the period January 1, 2013 – October 17, 2013.

3. Form 499 Filer ID: **803649, 803655, 803652, 804816, 803652, 804993, 819828, and FRN: 0005464284**
4. Name of signatory: **Matthew L. Dosch**
5. Title of signatory: **Senior Vice President of External Affairs**
6. Certification:

I, Matthew L. Dosch, 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 _____



Attachments: Accompanying Statement explaining CPNI procedures

Comporium, Inc. – FCC 499 Filer ID: 803649
Fort Mill Telephone Company – FCC 499 Filer ID: 803655
Lancaster Telephone Company – FCC 499 Filer ID: 803652
Citizens Telephone Company – FCC 499 Filer ID: 804816
Community Long Distance Company – FCC 499 Filer ID: 804993
Springboard Telecom, LLC– FCC 499 Filer ID: 819828
Comporium Wireless, LLC– FRN: 0005464284

P O. Box 470, Rock Hill, South Carolina 29731

STATEMENT OF FCC CPNI RULE COMPLIANCE

This statement serves to explain how Comporium, Inc. and its affiliated companies, Fort Mill Telephone Company (d/b/a "Comporium Communications"), Lancaster Telephone Company (d/b/a "Comporium Communications"), Citizens Telephone Company (d/b/a "Comporium Communications"), Community Long Distance, Inc. (d/b/a "Comporium Communications"), Springboard Telecom, LLC and Comporium Wireless, LLC (collectively the "Company") is complying with Federal Communications Commission ("FCC") rules related to the privacy of customer information. The type of information for which customer privacy is protected by the FCC's rules is called "customer proprietary network information" ("CPNI"). The FCC's rules restricting telecommunication company use of CPNI are contained at Part 64, Subpart U of the FCC's rules (47 C.F.R. §§ 64.2000-2009).

1. Identification of CPNI

The Company has in place and maintains customer service order management systems, inter-workgroup coordination procedures, additional support materials for employees, and continues to train applicable employees having access to, or occasion to use customer data, to identify what customer information is CPNI consistent with the definition of CPNI under the FCC's rules at Part 64, Subpart U, Section 64.2003(d) and Section 222(f)(1) of the Communications Act of 1934 as amended (47 U.S.C. § 222(f)(1)).

2. Identification of Services Affected by CPNI Rules

The Company has in place and maintains customer accounts, customer service order management systems, inter-workgroup coordination procedures, support materials for employees, and continues to train applicable employees to recognize the different types of telecommunications and non-telecommunications services that affect how the Company uses CPNI.

3. Identification of Permissible Uses of CPNI without Customer Authorization

The Company has established and continues to maintain inter-workgroup coordination procedures, support materials for employees, and trains applicable employees having access to, or occasion to use CPNI, to identify uses of CPNI not requiring customer authorization under the FCC's Part 64, Subpart U, Section 64.2005.

4. Identification of Uses of CPNI Requiring Customer Authorization

The Company has established and continues to maintain inter-workgroup coordination procedures, support materials for employees, and trains applicable employees having access to, or occasion to use CPNI, to identify uses of CPNI requiring customer authorization under the FCC's rules at Part 64, Subpart U, Section 64.2007.

5. Customer Notification and Authorization Process

The Company has established and continues to maintain inter-workgroup coordination procedures between relevant departments and trains employees responsible for obtaining customer authorization to use CPNI for marketing purposes, regarding the notice and approval requirements under the FCC's Part 64, Subpart U CPNI rules. FCC's CPNI rules at Part 64, Subpart U, Section 64.2008. The Company has complied with the notice requirements for Opt-Out approval. The Company does not provide CPNI to other parties and thus has not used the opt-in approval process.

6. Record of Customer CPNI Approval/Non-Approval

The Company has developed and utilizes a system of indicators for maintaining a readily accessible record of whether and how a customer has responded to Opt-Out approval within our service order management system as required by Section 64.2009(a) of the FCC's Part 64, Subpart U CPNI rules.

7. Disciplinary Process

The Company has in place an express disciplinary process to address any unauthorized use of CPNI where the circumstances indicate authorization is required under the FCC's Part 64, Subpart U CPNI rules.

8. Supervisory Review Process for Outbound Marketing

The Company has established and continues to utilize a supervisory review process regarding its compliance with the rules in Part 64, Subpart U, for outbound marketing situations. Prior to any outbound marketing effort, sales personnel must obtain supervisory approval of the proposed outbound marketing use. Any approval of CPNI use for outbound marketing efforts is limited to CPNI not requiring prior customer authorization or, where prior customer authorization is required, CPNI of customers having given the Company prior approval. The Company maintains records of its compliance for a minimum of one year.

02/03/2014

Delivered via Email to GK764P@att.com

Ms. Georgia Kruse
Director – Project Management
International, Alliances & Integrations
AT&T Mobility Services LLC

RE: Sub-Certification for CPNI Reporting Year 2013

Dear Ms. Kruse:

I, Matthew L. Dosch, certify that I am an officer of Comporium Wireless, LLC (the "company"), 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.*

On October 18, 2013, AT&T closed on an agreement with company to create a Limited Liability Company managed and controlled by AT&T to provide wireless services in several non-contiguous counties (or partial counties) in South Carolina (the "Property"). Company and AT&T contributed assets in exchange for equity interests in the LLC.

From October 18, 2013 to December 31, 2013, company continued to operate the Property and sell its wireless services under company's brand while AT&T began to migrate customers to AT&T service. During this time period, AT&T also received additional support services from company pursuant to a transition services agreement ("TSA"). Company remained compliant with the Commission's CPNI rules and the company's CPNI practices and procedures for the CPNI reporting period ending December 31, 2013.

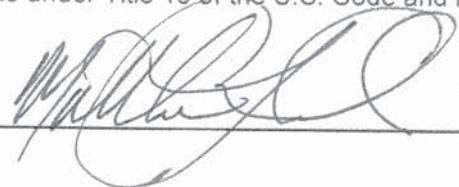
Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001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



Attachments: Accompanying Statement explaining CPNI procedures

Comporium Wireless, LLC– FRN: 0005464284

P O. Box 470, Rock Hill, South Carolina 29731

STATEMENT OF FCC CPNI RULE COMPLIANCE

This statement serves to explain how Comporium Wireless, LLC (the "Company") is complying with Federal Communications Commission ("FCC") rules related to the privacy of customer information. The type of information for which customer privacy is protected by the FCC's rules is called "customer proprietary network information" ("CPNI"). The FCC's rules restricting telecommunication company use of CPNI are contained at Part 64, Subpart U of the FCC's rules (47 C.F.R. §§ 64.2000-2009).

1. Identification of CPNI

The Company has in place and maintains customer service order management systems, inter-workgroup coordination procedures, additional support materials for employees, and continues to train applicable employees having access to, or occasion to use customer data, to identify what customer information is CPNI consistent with the definition of CPNI under the FCC's rules at Part 64, Subpart U, Section 64.2003(d) and Section 222(f)(1) of the Communications Act of 1934 as amended (47 U.S.C. § 222(f)(1)).

2. Identification of Services Affected by CPNI Rules

The Company has in place and maintains customer accounts, customer service order management systems, inter-workgroup coordination procedures, support materials for employees, and continues to train applicable employees to recognize the different types of telecommunications and non-telecommunications services that affect how the Company uses CPNI.

3. Identification of Permissible Uses of CPNI without Customer Authorization

The Company has established and continues to maintain inter-workgroup coordination procedures, support materials for employees, and trains applicable employees having access to, or occasion to use CPNI, to identify uses of CPNI not requiring customer authorization under the FCC's Part 64, Subpart U, Section 64.2005.

4. Identification of Uses of CPNI Requiring Customer Authorization

The Company has established and continues to maintain inter-workgroup coordination procedures, support materials for employees, and trains applicable employees having access to, or occasion to use CPNI, to identify uses of CPNI requiring customer authorization under the FCC's rules at Part 64, Subpart U, Section 64.2007.

5. Customer Notification and Authorization Process

The Company has established and continues to maintain inter-workgroup coordination procedures between relevant departments and trains employees responsible for obtaining customer authorization to use CPNI for marketing purposes, regarding the notice and approval requirements under the FCC's Part 64, Subpart U CPNI rules. FCC's CPNI rules at Part 64, Subpart U, Section 64.2008. The Company has complied with the notice requirements for Opt-Out approval. The Company does not provide CPNI to other parties and thus has not used the opt-in approval process.

6. Record of Customer CPNI Approval/Non-Approval

The Company has developed and utilizes a system of indicators for maintaining a readily accessible record of whether and how a customer has responded to Opt-Out approval within our service order management system as required by Section 64.2009(a) of the FCC's Part 64, Subpart U CPNI rules.

7. Disciplinary Process

The Company has in place an express disciplinary process to address any unauthorized use of CPNI where the circumstances indicate authorization is required under the FCC's Part 64, Subpart U CPNI rules.

8. Supervisory Review Process for Outbound Marketing

The Company has established and continues to utilize a supervisory review process regarding its compliance with the rules in Part 64, Subpart U, for outbound marketing situations. Prior to any outbound marketing effort, sales personnel must obtain supervisory approval of the proposed outbound marketing use. Any approval of CPNI use for outbound marketing efforts is limited to CPNI not requiring prior customer authorization or, where prior customer authorization is required, CPNI of customers having given the Company prior approval. The Company maintains records of its compliance for a minimum of one year.

Annual 64.2009 € CPNI Certification for 2013

Date filed: January 23, 2014

Horry Telephone Cooperative, Inc.

Form 499 Filer ID: 806994

Name of signatory: Glenda L. Page

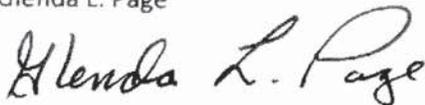
Title of signatory: Chief Executive, Human Resources

I, Glenda L. Page, certify that I am an executive of Horry Telephone Cooperative, Inc. ("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 Federal Communications Commission (Commission) Customer Proprietary Network Information ("CPNI") rules. Attached to this certificate is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 of the Commission's rules.

In the past year, the Company has not taken any action against data brokers. The Company does not share CPNI among its affiliates, unless prior customer approval has been obtained or no customer approval is needed. Furthermore, the Company requires all independent contractors granted access to CPNI to enter into an appropriate confidentiality agreement and to abide by applicable laws, regulations, policies, and procedures. The Company does not disclose CPNI to other third parties except as requested by the customer or as compelled or authorized by law.

The Company has not received any substantiated customer complaints in the past year concerning the unauthorized release of CPNI. The Company notifies customers of their rights to restrict access to, use of, and disclosure of their CPNI. Periodic notices and one-time notices are provided to customers as appropriate. Such notices may be provided through multiple methods including bill inserts, customer newsletters, notices published in the telephone directory, notices included on the Company's website, and notices provided during telephone contact. The Company maintains records of all notices and approvals for not less than one year.

Glenda L. Page



Chief Executive - Human Resources
Horry Telephone Cooperative, Inc.

Attachment

Steps Taken By Company to Ensure the Confidentiality of CPNI Records

Horry Telephone Cooperative, Inc. Policy G-34 includes the CPNI Guidelines as listed below.

1. Failure by an employee to abide by the applicable CPNI policies and procedures is cause for discipline, up to and including employment termination.
2. All Company employees during their annual Human Resources Policy review receive an overview of CPNI requirements. (Training rosters are available upon request).
3. All customer-interfacing employees are required to attend CPNI training prior to receiving access to customers' CPNI call detail information. (Training rosters are available upon request).
4. Only job positions with a business need to know are given access to CPNI call detail records.
5. A process is in place for reporting CPNI breaches and includes the completion of an "Incident Report Form."
6. A process is in place for researching and validating CPNI claims.
7. A Company security officer is responsible for investigating reported CPNI breaches.
8. During annual employee performance reviews, employees are reminded of CPNI policy with each employee acknowledging, in writing, his/her understanding of and consent to CPNI rules and procedures.
9. Procedures are in place for the appropriate disposal of CPNI records.
10. Security restrictions are placed on the mailing of CPNI records.

January 14, 2014

Delivered via Email to GK764P@att.com

Ms. Georgia Kruse
Director – Project Management
International, Alliances & Integrations
AT&T Mobility Services LLC

RE: Sub-Certification for CPNI Reporting Year 2013

Dear Ms. Kruse:

I, Glenda L. Page, certify that I am an executive of Horry Telephone Cooperative, Inc. ("Company"), 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 Customer Proprietary Network Information (CPNI) rules. Attached to this certificate is an accompanying statement explaining how the Company's procedures ensure that the Company is in compliance with the requirements set forth in section 64.2001 of the Commission's rules.

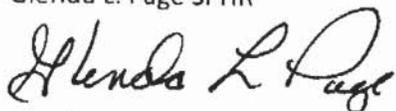
On October 18, 2013, AT&T closed on an agreement with Company to create a Limited Liability Company managed and controlled by AT&T to provide wireless services in several non-contiguous counties (or partial counties) in South Carolina (the "Property"). Company and AT&T contributed assets in exchange for equity interests in the LLC.

From October 18, 2013 to December 31, 2013, Company continued to operate the Property and sell its wireless services under Company's brand while AT&T began to migrate customers to AT&T service. During this time period, AT&T also received additional support services from Company pursuant to a transition services agreement ("TSA"). Company remained compliant with the Commission's CPNI rules and the Company's CPNI practices and procedures for the CPNI reporting period ending December 31, 2013.

In the past year, the Company has not taken any action against data brokers. The Company does not share CPNI among its affiliates, unless prior customer approval has been obtained or no customer approval is needed. Further, the Company requires all independent contractors who have obtained access to CPNI to enter into an appropriate confidentiality agreement and to abide by applicable laws, regulations, policies, and procedures. The Company does not disclose CPNI to other third parties except as requested by the customer or as compelled or authorized by law.

The Company has not received any substantiated customer complaints in the past year concerning the unauthorized release of CPNI. The Company notifies customers of their rights to restrict access to, use of, and disclosure of their CPNI. Periodic notices and one-time notices are provided as appropriate. Such notices may be provided through multiple methods including bill inserts, customer newsletters, notices published in the telephone directory, notices included on the Company's website, and notices provided during telephone contact. HTC maintains records of all notices and approvals for not less than one year.

Glenda L. Page SPHR

A handwritten signature in cursive script that reads "Glenda L. Page".

Chief Executive - Human Resources
Horry Telephone Cooperative, Inc.

Attachment

Steps Taken By Company to Ensure the Confidentiality of CPNI Records

Horry Telephone Cooperative, Inc. Policy G-34 includes the CPNI Guidelines as listed below.

1. Failure by an employee to abide by the applicable CPNI policies and procedures is cause for discipline, up to and including employment termination.
2. All Company employees during their annual Human Resources Policy review receive an overview of CPNI requirements. (Training rosters are available upon request).
3. All customer-interfacing employees are required to attend CPNI training prior to receiving access to customers' CPNI call detail information. (Training rosters are available upon request).
4. Only job positions with a business need to know are given access to CPNI call detail records.
5. A process is in place for reporting CPNI breaches and includes the completion of an "Incident Report Form."
6. A process is in place for researching and validating CPNI claims.
7. A Company security officer is responsible for investigating reported CPNI breaches.
8. During annual employee performance reviews, employees are reminded of the CPNI policy with each employee acknowledging, in writing, his/her understanding of and consent to CPNI rules and procedures.
9. Procedures are in place for the appropriate disposal of CPNI records.
10. Security restrictions are placed on the mailing of CPNI records.

EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013 OF WILLIAM HAGUE, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY AND CONSUMER MARKETS – INTERNATIONAL, ALLIANCES AND INTEGRATION

Schedule E: Element Mobile Property

In accordance with Section 64.2009(e) of the CPNI rules, AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) has adopted procedures that are intended to ensure the compliance of the Element Mobile Property, as defined below, with the FCC’s CPNI rules. This statement summarizes and explains the procedures and explains how these procedures were designed and adopted to ensure compliance with the CPNI rules.

On December 6, 2013, New Cingular Wireless PCS, LLC, by its Manager AT&T Mobility Corp, (“AT&T”) closed on a Contribution and Formation Agreement with the Wisconsin RSA #7 Limited Partnership and its individual partners, d/b/a Element Mobile (“Seller”), forming Lake Mobility LLC. Lake Mobility LLC is majority owned and managed by AT&T and will provide wireless services in Wood, Portage, Waupaca, Juneau, Adams, Marquette, Green Lake, and Waushara counties in Wisconsin. The Seller contributed its Wisconsin spectrum licenses, network assets, retail stores and approximately 46,000 wireless subscribers (the “Element Mobile Property”) to Lake Mobility LLC. During December 6, 2013 to December 31, 2013 (the “Time Period”), AT&T operated the Element Mobile Property under the Element Mobile brand. During the Time Period, AT&T received certain support services from Seller pursuant to a transition services agreement (“TSA”).

This Statement addresses AT&T’s operation of the Element Mobile Property during the Time Period. This Statement is based and relies on the following:

- (1) ACPNI Certification filed by Seller with the FCC on January 21, 2014 (“Seller Certification”) which states that during calendar year 2013, Seller established operating procedures that are adequate to ensure the Element Mobile Property’s compliance with the requirements of the FCC’s CPNI rules (“Legacy Sales Practices”).
- (2) A CPNI Subcertification dated February 10, 2014, by Seller which states that during the Time Period, Seller continued the Legacy Sales Practices in its provision of services to AT&T under the TSA.

A. Customer CPNI Approvals. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

B. Training and Discipline. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

C. CPNI Complaints and Breaches. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

D. Security and Authentication. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

Date:

William W. Hague
William Hague



Law Offices of Bennet & Bennet, PLLC

Maryland

6124 MacArthur Boulevard
Bethesda, Maryland 20816
Tel: (202) 371-1500
Fax: (202) 371-1558
www.bennetlaw.com

District of Columbia

10 G Street NE, Suite 710
Washington, DC 20002

Caressa D. Bennet
Michael R. Bennet
Marjorie G. Spivak*
Kenneth C. Johnson‡
Howard S. Shapiro

* Admitted in DC & PA Only
‡Admitted in DC & VA Only

Daryl A. Zakov^
Robert A. Silverman
Anthony K. Veach*
Erin P. Fitzgerald
Of Counsel
Tara B. Shostek

^Admitted in DC & WA Only
#Admitted in DC & FL Only

January 31, 2014

Via ECFS

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

Re: CPNI Certification and Accompanying Statement
EB Docket No. 06-36

Dear Ms. Dortch:

Wisconsin RSA #7 Limited Partnership d/b/a Element Mobile (“the Company”), by its attorneys and pursuant to Section 64.2009(e) of the Commission’s Rules, hereby submits its annual Customer Proprietary Network Information (CPNI) certification and accompanying statement.

Should you have any questions or need further information, please contact the undersigned.

Sincerely,

/s/

Marjorie Spivak

cc: Best Copy and Printing, Inc.

Attachments

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

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2014 covering the prior calendar year 2013

1. Date filed: January 21, 2014
2. Name of company(s) covered by this certification: Wisconsin RSA #7 Limited Partnership dba Element Mobile
3. Form 499 Filer ID: 802302
4. Name of signatory: Gregory A. Aymar
5. Title of signatory: COO
6. Certification:

I, Gregory A. Aymar, 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 in the past year.

The company received one customer complaint in the past year concerning the unauthorized release of CPNI by an employee to an unauthorized person. The company investigated the complaint and determined that no information was disclosed and that no breach had occurred.

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  _____, as agent of the carrier

Attachments: Accompanying Statement explaining CPNI procedures

CPNI Usage Policy Statement

Pursuant to Section 64.2009(e) of the Federal Communications Commission's ("FCC") rules, this statement explains how Wisconsin RSA #7 Limited Partnership dba Element Mobile's (the "Company") operating procedures ensure compliance with Part 64, Subpart U of the FCC's rules.

Company CPNI Policies

The Company has chosen to prohibit the use of CPNI for marketing purposes by itself and between its affiliates.

The Company's CPNI Policy Manual includes an explanation of what CPNI is and when it may be used without customer approval.

Employees with access to CPNI have been trained as to when they are and are not authorized to use CPNI. The Company's CPNI Policy Manual describes the disciplinary process related to noncompliance with CPNI obligations, and sets forth the penalties for non-compliance, which can include termination of employment.

The Company has established a supervisory review process regarding Company compliance with the FCC's CPNI rules.

The Company requires affirmative written/electronic subscriber request for the release of CPNI to third parties.

Company's CPNI Safeguards

A Corporate Officer has been named as the CPNI Compliance Officer and is held responsible for annually certifying that the Company is in compliance with the FCC's CPNI rules and submitting the certification and an accompanying statement explaining how Company complies with the FCC's CPNI rules to the FCC prior to March 1.

The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Company authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact, online account access, or an in-store visit.

The Company only discloses call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information or account information. If a customer does not provide a password, Company only discloses call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the customer is able to provide call detail information during a customer-initiated call without Company's assistance, then Company is permitted to discuss the call detail information provided by the customer.

The Company has established a system of passwords and password protection. For a new customer, Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, Company must first authenticate the customer without the use of readily available biographical information or account information. Company authenticates a customer using non-public information such as calling the customer at the telephone number of record or using a Personal Identification Number (PIN) method to authenticate a customer.

For accounts that are password protected, Company cannot obtain the password by asking for readily available biographical information or account information to prompt the customer for his password.

A customer may access call detail information by establishing an online account or by visiting a carrier's retail location. If a password is forgotten or lost, Company uses a back-up customer authentication method that is not based on readily available biographical information or account information.

If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking Company to send the call detail information to an address of record or by the carrier calling the telephone number of record.

Company password-protects online access to all CPNI, call detail and non-call detail. Company provides customers with access to CPNI at a carrier's retail location if the customer presents a valid photo ID and the valid photo ID matches the name on the account. Company has procedures and policies in place to notify a customer immediately when 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 through a carrier-originated voicemail or text message to the telephone number of record, or by mail to the address of record.

In the event of a CPNI breach, Company complies with the FCC's rules regarding notice to law enforcement and customers. Company maintains records of any discovered breaches and notifications to the United States Secret Service (USSS) and FBI regarding those breaches, as well as the USSS and the FBI response to the notifications for a period of at least two year.

Actions Taken Against Data Brokers and Customer Complaints

Company has taken no actions against data brokers in the last year. The Company received one customer complaint in the past year concerning the unauthorized release of CPNI by an employee to an unauthorized person. The company investigated the complaint and determined that no information was disclosed and that no breach had occurred.

Your submission has been accepted

ECFS Filing Receipt - Confirmation number: 2014131256575

Proceeding

Name	Subject
06-36	CPNI Compliance Certification Annual Filing

Contact Info

Name of Filer: Wisconsin RSA #7 Limited Partnership
d/b/a Element Mobile
Email Address: mgspivak@bennetlaw.com
Attorney/Author Name: Marjorie Spivak
Lawfirm Name (required if represented by counsel): Bennet & Bennet, PLLC

Address

Address For: Law Firm
Address Line 1: 6124 MacArthur Boulevard
City: Bethesda
State: MARYLAND
Zip: 20816

Details

Small Business Impact: NO
Type of Filing: STATEMENT

Document(s)

File Name	Custom Description	Size
Element 2014 CPNI FINAL.pdf		260 KB

Disclaimer

This confirmation verifies that ECFS has received and accepted your filing. However, your filing will be rejected by ECFS if it contains macros, passwords, redlining, read-only formatting, a virus, or automated links to other documents.

Filings are generally processed and made available for online viewing within one business day of receipt. You may use the link below to check on the status of your filing:

<http://apps.fcc.gov/ecfs/comment/confirm?confirmation=2014131256575>

For any problems please contact the Help Desk at 202-418-0193.

Wisconsin RSA #7 Limited Partnership dba Element Mobile
CPNI Certification to AT&T Mobility LLC
Calendar Year 2013

Date: February 10, 2014

During the period from December 6, 2013-December 31, 2013, Wisconsin RSA #7 Limited Partnership dba Element Mobile ("Element") provided AT&T Mobility LLC ("AT&T") with certain Transition Services for the Element markets acquired by AT&T. Under Section ___ of the Transition Services Agreement, each party is required to comply with the provisions of federal laws that may be applicable to its performance of such transition services. {NOTE: need TSA so I can properly describe and format}

I, Al Aymar, Chief Operating Officer, certify, based upon my own personal knowledge and the personal knowledge of subject matter experts upon whom I have reasonably relied in making this certification, that Element has established operating procedures as part of its provision of Transition Services for AT&T that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. 64.2001 et seq.

Signature: _____

EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013 OF WILLIAM HAGUE, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY AND CONSUMER MARKETS – INTERNATIONAL, ALLIANCES AND INTEGRATION

Schedule F: Long Lines Wireless Property

In accordance with Section 64.2009(e) of the CPNI rules, AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) has adopted procedures that are intended to ensure the compliance of the Long Lines Wireless Property, as defined below, with the FCC’s CPNI rules. This statement summarizes and explains the procedures and explains how these procedures were designed and adopted to ensure compliance with the CPNI rules.

On December 20, 2013, AT&T closed on its acquisition of certain wireless assets of Long Lines Wireless (“Seller”). The acquisition included Seller’s spectrum licenses and network assets in Iowa, Nebraska, Minnesota, South Dakota, and North Dakota, and approximately 10,500 wireless subscribers in Iowa (the “Long Lines Wireless Property”). During December 20, 2013, to December 31, 2013 (the “Time Period”), AT&T Mobility operated the Long Lines Wireless Property under the Long Lines Wireless brand. During the Time Period, AT&T received certain support services from Seller pursuant to a transition services agreement (“TSA”). This Statement addresses AT&T’s operation of the Long Lines Wireless Property during the Time Period. This Statement is based and relies on the following:

- (1) A CPNI Certification filed by Seller with the FCC on January 10, 2014 (“Seller Certification”) which states that during its operation of the Long Lines Wireless Property in 2013, Seller established operating procedures that are adequate to ensure the Long Lines Wireless Property’s compliance with the requirements of the FCC’s CPNI rules procedures (“Legacy Sales Practices”).
- (2) A CPNI Certification filed by Seller with the FCC on January 10, 2014, which states that during the Time Period, Seller continued the Legacy Sales Practices in the provision of services to AT&T under the TSA during the Time Period (the “TSA Certification”).

A. Customer CPNI Approvals. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

B. Training and Discipline. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

C. CPNI Complaints and Breaches. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

D. Security and Authentication. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

Date: William W. Hague
William Hague

January 10, 2014

Federal Communications Commission
445 12th Street, SW
Suite TW-A325
Washington, D.C 20554

RE: EB docket 06-36
Annual CPNI Certification for the Year 2013

In accordance with Public Notice DA 09-9 attached is the annual CPNI certification filing for the year of 2013, pursuant to 47 C.F.R 64.2009(e), for Long Lines and affiliate companies.

Sincerely,

A handwritten signature in black ink, appearing to read "Jason Kvidera", with a long horizontal flourish extending to the right.

Jason Kvidera
Financial Manager
CPNI Compliance Officer

January 10, 2014

Dear Federal Communications Commission,

Enclosed is the 2013 CPNI Filing for Long Lines and its affiliate companies. Long Lines is the parent company for the following telecommunication providers:

- Northwest Iowa Telephone Company
- Jordan-Soldier-Valley Telephone Company
- Jefferson Telephone Company
- Advanced Network Communications
- Mapleton Communications
- Orange City Communications
- Long Lines Metro
- Long Lines Siouxland
- Long Lines Wireless

The above companies were trained and certified by the Long Lines Compliance Officer and follow Long Lines' CPNI rules, regulations, and procedures.

If you have any questions regarding any of the affiliate companies or need additional information, please feel free to contact me at 712.271.4000.

Sincerely,



Jason Kvidera
Compliance Officer

Annual 47 C.F.R 64.2013(e) CPNI Certification
EB Docket 06-36

Annual 64.2013(e) CPNI Certification for 2013

Date Filed: January 10, 2014

Name of Company covered by this certification: Long Lines and affiliate companies

Form 499 Filer ID: 826537 (Long Lines Wireless)

Name of Signatory: Jason Kvidera

Title of Signatory: Financial Manager, Compliance Officer

I, Jason Kvidera, certify that I 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 set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commissions against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPN.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or 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).

The company represents and warrants that the above certification in consistent with 47.C.F.R 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that the 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



What is CPNI?

CPNI stands for Customer Proprietary Network Information

The *Gist* of CPNI:

- Protect the customer's privacy
- Market products and services within the existing customer relationship
- Do not use customer information to *target* customers
- Do not give customer information to other companies

Types of CPNI:

Call Detail Records

- Require greatest protection of privacy!

Purchases

- LD PIC codes, video, Internet, wireless, features

General Account Information

- Name, address

Acceptable uses of CPNI

- Exchange of customer information for the purpose of inter-carrier billing
- Marketing of services within an existing customer relationship
- Mass Marketing such as bill notices, bill inserts, direct mail, in-house telemarketing, newsletter articles, advertising, signage
- Law enforcement
- Directory listings
- Service provisioning by independent contractors (overbuild projects)
- In-house mailings
- Provisioning of customer service, products and services (cable modems, etc)
- Protecting telco property (peds, boxes on outside of homes)

Restrictions of CPNI

- Selling or distributing of CPNI to a third party without customer approval
- Selling or distributing CPNI to a joint-venture partner or independent contractor without the customer's express permission (opt-in)
- Win-back campaigns that use information about a customer's relationship with a competitor to target that customer.
- Targeted-marketing without giving the customer an opt-out opportunity
- Discussing Call Detail Records without a password
- Providing CPNI to mail houses, telemarketers, or direct mailing firms (data brokers)

August 2007



MARKETING/SALES

**CPNI impacts all employees that have access to customer records including customer service, sales, marketing, accounting, and install and repair staff.

Marketing and CPNI

- Review ALL marketing efforts with the CPNI Compliance Officer
- Conduct as much mass marketing as possible
- Avoid target mailings. When targeting, observe the rules.

Telemarketing:

- If conducted in-house (which Long Lines does), it requires no sharing of CPNI with a third party or independent contractor
- Do NOT give target telephone numbers to telemarketing firms
- It is OK to give ALL phone numbers to telemarketing firms

Winbacks:

- It is OK to generate a list of disconnected customers and attempt to win-back.
- It is NOT OK to use port requests or cancellation codes to target competitors' customers

Websites:

- General Information on the website is not targeted and is OK.
- Account information must be password protected



Opt-in and Opt-out forms

Opt-in: Express written consent to receive marketing materials and sales communications about products and services outside the customer relationship or express written consent to share customer information with third parties, joint venture partners, and independent contractors.

Long Lines will not be using the Opt-In process.

Opt-out: Express written consent to be excluded from marketing materials and sales communications about products and services outside the existing customer relationship.

Opt-Out Process

- Mail form to all customers notifying them that "from time to time Long Lines may use your account information to promote additional products and services available from us."
- Provide the customer the option of "opting out" by signing and returning the opt-out form, or a request can be made verbally.
- Must allow 32 days to receive opt-out forms
- Note the customer records of each opt-out
- Screen opt-outs from all future *targeted* marketing.
- Secure and store opt-out requests in the Long Lines CPNI files.
- New Customers: Opt-out notice will be sent after 1st month

* Communication on bills 1x per year letting customers know how to opt out

August 2007



Bill Notification

The following notification will be sent to every new customer at the end of each month. Existing customers will be notified every 2 years. - LL does every year

Long Lines respects your privacy and observes the privacy rules established by the Federal Communications Commission, the State Public Utility Commission and other telecom oversight agencies.

Long Lines will never sell your account information or provide details of your telephone calls to other parties, unless required by law enforcement.

From time to time, we would like to notify you of additional products available from us outside the existing business relationship we have with you. For example, if you have our local phone service, you may be interested to learn about specials on our cable and wireless services. However, you have the right to be excluded from these marketing campaigns.

If it is acceptable to receive information about additional products and services, you need do nothing. However, if you prefer to be excluded from these marketing efforts, please call our office at 1.866.537.5900, and we will screen you from all targeted marketing programs for the next two years.

Thank you for being a Long Lines customer.

August 2007



CUSTOMER SERVICE

CPNI in Everyday Operations

Customer Service—5 things to remember

1. Authenticate **every** customer
2. A password is **required** for Call Detail Records
3. Check customer's opt-out status (pop-up screen will appear)
4. Ask permission to discuss products and services ("while I have you on the phone...")
5. Aggressively upsell

Technicians-2 things to remember

1. Sell within existing customer relationship
2. Or, ask permission to discuss additional products and services
"I know I'm here to fix your phone service, but may I tell you about some new services we offer?"



Customer Authentication and Password Procedures

Customer Authentication

Every customer is required to be authenticated before details on the account are discussed.---This is to prevent pretexting. **Pretexting** is when an imposter contacts the telephone company claiming to be a customer in order to obtain call detail records or account information.

Customer Authentication Script:

To establish a password:

"I'd be happy to help you. Could you please verify the name on your account? Could you please confirm your average monthly bill?—The Federal Communications Commission now requires us to use passwords to access your account. At this time, I would like to set up a password to further protect your privacy. Could you please give me a password you would like to use on your account? We'd also like to establish a backup question.

Back-up Questions

The following questions will be used as the back-up question. The customer needs to answer only one.

- 1) What are the last 4 digits of your social security number?
- 2) What is your mother's maiden name?
- 3) What is your childhood street name?

(If customer declines to establish a password): "I can understand that you do not want to track a password. To provide your account information, I can call you back at the telephone number we have associated with your account or you can stop by the office and present a government-issued ID, such as a driver's license, to receive the information."

If password is already established:

"I'd be happy to help you. Could you please verify the name on your account? Could you please verify the password on your account?"



Password Procedures

Passwords **must** be used to share call detail records, although Long Lines will obtain a password for all account information. Employees are forbidden from supplying call detail records to a customer making an in-bound call to the office, even if the caller ID indicates that the customer is calling from the telephone number of record.

If the customer is unable to supply the password or refuses to establish a password, the employee may share call detail records by:

1. Calling the customer back at the telephone number of record
2. Mailing or emailing the call detail record to the address (physical or email) of record
3. Confirming the customer's identity in person with a valid, government-issued ID

**If the customer supplies the call detail record for a particular call in question, the employee may confirm the call detail record, but only for that call. Other call detail records may not be supplied without a password, or without the customer first providing the information.

The employee can help the customer remember passwords with back-up questions that are not based on readily available information such as social security number, childhood pet, etc. ---**However, if these questions are used to prompt the customer's memory, the FCC requires the phone company to provide notification to the address of record that the back-up questions were used to gain account access.**

How to establish a password:

1. Call the customer at the telephone number of record or authenticate the customer without the use of readily available information or account information.
2. Have the customer select a password 4-12 digits containing letters and numbers and establish a back-up question
3. Store the password with the customer's account
4. Provide online option for online billing, if applicable

The following questions will be used as the back-up question. The customer needs to answer only one.

- 1) What are the last 4 digits of your social security number?
- 2) What is your mother's maiden name?
- 3) What is your childhood street name?



August 2007

Notification of Account Change

The customer must receive a written notification within 48 hours of the following account changes:

- Password Change (a new password is created or changed)
- Address of Record Change
- New address of record created
- Lost or forgotten password (back up questions were used to re-issue a lost or forgotten password)
- On-line account creation
- On-line account change
- A security breach has occurred

(THIS NOTIFICATION LETTER WILL BE MADE AVAILABLE ELECTRONICALLY)

Dear Long Lines Customer,

This letter is to notify you of the following changes made to your account on

(date).

The following change/s has been made:

- _____ Password Change
- _____ Address of Record Change
- _____ New address of record created
- _____ Lost of forgotten password
- _____ Online account creation
- _____ Online account change

Description of Change:

If you have any questions regarding your account, please feel free to call our office at 1-866-537-5900.

Sincerely,

Long Lines Customer Care Department

UPSELLING

When upselling use the “safety net” approach by asking permission to review the customer’s account information and discuss additional products and services.

Safety Net Example:

“May I have permission to review your account and discuss services you might not currently be receiving from us?”

Other upselling examples:

“I see that you have caller ID. Did you know that with voicemail and call waiting, you can see who’s calling when you’re on the line, and let it ring to voicemail?”

“Would you like to add a premium channel package to your order?”

“I notice that you’re using dial-up Internet, have you heard about our specials on High Speed Internet?”

UPSELLING

Already Purchase and Calling About	OK to Sell	Outside of Existing Customer Relationship
Local Exchange	Calling features, Second Lines, CPE, Key Systems	Long Distance, VoIP, High-speed Internet, Video, Wireless
Long Distance	More Minutes, Alternative Long Distance Plans, Unlimited Switched Long Distance	Local Voice, VoIP, High-speed Internet, Wireless, Video
Dial-up Internet	High-speed Internet*, CPE, Routers, Modems, Spam Filtering, Virus Protection, Mailboxes, Static IP Addresses, Web Storage	Local Voice, Long Distance, VoIP, Video, Wireless
High-speed Internet	VoIP, Greater Bandwidth, CPE, Routers, Modems, Spam Filtering, Virus Protection, Mailboxes, Static IP Addresses, Web Storage	Local Voice, Long Distance, Video
Wireless	Handsets, Expanded Service Plans, Accessories, Additional Users, Data, Text Messaging, Minutes of Use, Wireless Broadband	Local Voice, Long Distance, Video
Video	Premium Channels, DVR, VoD, HD, Digital Tiers, CPE, High-speed Internet*, Pay-per View	Local Voice, Long Distance
Triple Play	VoIP, Premium Channels, DVR, VoD, HD, Digital Tiers, CPE, High-speed Internet*, Pay-per-view, Greater Bandwidth, CPE, Routers, Modems, Spam Filtering, Virus Protection, Mailboxes, Static IP Addresses, Web Storage, Calling Features, Second Lines, CPE, Key Systems	Wireless
Quad Play	VoIP, Premium Channels, DVR, VoD, HD, Digital Tiers, CPE, High-speed Internet*, Pay-per-view, Greater Bandwidth, CPE, Routers, Modems, Spam Filtering, Virus Protection, Mailboxes, Static IP Addresses, Web Storage, Calling Features, Second Lines, CPE, Key Systems, Wireless (Handsets, Expanded Service Plans, Accessories, Additional Users, Data, Text Messaging, Minutes of Use, Wireless Broadband)	Nothing



Reporting Procedures for CPNI Violations and Breaches

- Notification to Law Enforcement:
- Notify Law Enforcement within 7 business days by electronic notification through the central reporting systems of the United States Secret Service (USSS) and the FBI
- Unless requested otherwise, after 7 days of notifying law enforcement, notify the customer of the CPNI breach
- Maintain records of any discovered breaches, notifications, and law enforcement response for 2 years. Include the date of discovery, date of law enforcement notification, detailed description of the CPNI that was breached, and circumstances of the breach.

**Law enforcement may request a delay in customer notification in order to investigate the CPNI breach. Long Lines will observe law enforcements requests, unless there is an urgent need to notify the customer to avoid immediate and irreparable harm. All requests by law enforcement to delay customer notification should be thoroughly documented.

August 2007



Employee Disciplinary Procedures

Employees might unintentionally violate CPNI rules by mentioning a product or service outside the existing relationship or by targeting a mailing without the Compliance Officer's review. The FCC requires carriers to adopt disciplinary actions for all CPNI violations, whether intentional or unintentional.

Unintentional Violations:

First Violation: Retrained and recertified

Second Violation: Laid-off or terminated (decision to be made by Compliance Officer and Supervisor)

Intentional Violations:

For intentional violations, such as distribution of CPNI to third parties for financial gain, to harm the company, or to harm the customer, the breach will be reported and the employee will be terminated.

Section 222 of the 1996 Telecom Act

CPNI

Section 222 of the Telecom Act

“SEC. 222. PRIVACY OF CUSTOMER INFORMATION.

“(a) IN GENERAL.—Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

“(b) CONFIDENTIALITY OF CARRIER INFORMATION.—A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

“(c) CONFIDENTIALITY OF CUSTOMER PROPRIETARY NETWORK INFORMATION.—

“(1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS.—

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall use only, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

“(2) DISCLOSURE ON REQUEST BY CUSTOMERS.—A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

“(3) AGGREGATE CUSTOMER INFORMATION.—A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or person on reasonable and nondiscriminatory terms and conditions upon reasonable request therefore.

“(d) EXCEPTIONS.—Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—

“(1) to initiate, render, bill, and collect for telecommunications services;

“(2) 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;

or

“(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service.

“(e) SUBSCRIBER LIST INFORMATION.—Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under non discriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

“(f) DEFINITIONS.—As used in this section:

“(1) CUSTOMER PROPRIETARY NETWORK INFORMATION.—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 telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

“(2) AGGREGATE INFORMATION.—The term ‘aggregate customer information’ means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

“(3) SUBSCRIBER LIST INFORMATION.—The term ‘subscriber list information’ means any information—

“(A) identifying the listed names of subscribers of a carrier and such subscribers’ telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

“(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.”

August 2007



CPNI Employee Certification

I, the undersigned, hereby acknowledge receiving and reviewing Long Lines' CPNI Rules and Policies. I have completed the training coordinated by the Long Lines Compliance Officer. I further understand that I am responsible for understanding and observing Long Lines' CPNI policies and the rules established by the Federal Communications Commission and the Iowa/Nebraska/South Dakota Public Utilities Commission.

Finally, I accept responsibility for any violations of CPNI and the rules and understand the disciplinary procedures in place at Long Lines, which include termination.

Name _____

Position _____

Date CPNI Manual Received _____

Date of CPNI Training _____

Signature _____ Date _____

Witnessed by the CPNI Compliance Officer

Printed Name _____

Signature _____ Date _____

****COPY FOR YOUR RECORDS** **KEEP IN BOOKLET****

August 2007



Name and Contact Information of the CPNI Compliance Officer

Contact Information:

~~Jeff Donaldson~~
~~Stormie Westphal~~
712.271.6252
~~stormie.westphal@longlines.com~~
~~Jeff.Donaldson@longlines.biz~~

Duties of the Compliance Officer:

- This person is the central point of contact for employee, agents (attorneys, contractors, consultants, agents, vendors) and customers regarding the company's CPNI responsibilities
- Maintains and secures the company's CPNI files
- Tracks all customer CPNI complaints for one year
- Tracks all breaches of CPNI rules for two years
- Reviews and documents company use of CPNI



August 2007

FCC CPNI Rules

Complying with the FCC's CPNI rules is a seven step process:

- 1) Designate a Compliance Officer
- 2) Train and certify employees on CPNI requirements
- 3) Notify customers of any account changes
- 4) Notify law enforcement and customers of any unauthorized disclosure of CPNI
- 5) Establish disciplinary procedures for employee violations of CPNI rules
- 6) Take measures to discover and protect against pretexting and unauthorized disclosures of CPNI
- 7) File annual certification by March 1

1) **Designate a Compliance Officer**

- Central point of contact for employees, agents (attorneys, contractors, consultants, vendors) and customers regarding the company's CPNI responsibilities
- Maintains and secures the company's CPNI files
- Tracks all customer CPNI complaints for one year
- Tracks all breaches of CPNI rules for two years
- Reviews and documents company use of CPNI

2) **Train and certify employees on CPNI requirements**

All employees and agents with access to CPNI must:

- Receive and read the company's CPNI manual
- Sign the company's CPNI Policy Acknowledgment

Attend group or private training, supervised by the CPNI Compliance Officer

3) **Notify customers of any account changes**

*Customers must be notified immediately by mail to the address of record, or by voicemail, or text message to the telephone number of record, upon the following:

- A new password is created or changed
- The address of record is changed
- The online account of record is changed
- Back-up questions are used to re-issue a lost or forgotten password
- A security breach occurs

August 2007



- 4) Notify law enforcement and customers of any unauthorized disclosure of CPNI**
- Notify law enforcement within seven business days by electronic notification through the central reporting systems of the United States Secret Service and the FBI.
 - Unless requested otherwise, after seven business days of notifying law enforcement, notify the customer of the CPNI breach
 - Maintain records of any discovered breaches, notifications, and law enforcement response for two years. Include date of discovery, date of law enforcement, detailed description of the CPNI that was breached, and circumstances of the breach

5) Establish disciplinary procedures for employee violations of CPNI rules

- Reprimand
- Retrain
- Re-certify
- Escalated disciplinary actions for repeat offenses
- Intentional distribution of CPNI to other parties to harm Long Lines or for personal gain—termination

6) Take measures to discover and protect against pretexting and unauthorized disclosures of CPNI

- Guard against pretexting with measures beyond CPNI requirements, but consistent with Section 222, such as encryption and audit trails
- Detect pretexting
- Document actions

7) File annual certification by March 1

- Complete EB Docket No. 06-36
- Include explanations of any actions taken against data brokers
- Include a summary of all customer complaints
- File on or before March 1

FAQ ON THE CPNI RULES and PROCEDURES

Where is the CPNI password kept on the account?

Previous to Oct 2008 all of the CPNI passwords were kept on the contact screen of a customer's account.

After Oct 2008 all of the CPNI passwords and back up questions will be kept on the Profiler screen on the customer's account.

If a customer asks to Opt Out of CPNI what does that mean?

This means that the customer requests to be excluded from marketing materials and sales communications about product and services outside the existing customer relationship.

If a customer chooses to Opt Out you will select the appropriate box on the Profiler Screen in their account.

How do I establish a password?

Ask the customer to select a password that is 4 – 12 characters containing letters and/or numbers.

The password can not be the customer's Social Security Number.

Do I need to create a backup question for the customer?

Yes, the customer only needs to answer ONE back up question, however there will be situations when more than one question will need to be answered. (EX: The CCR does not feel they are speaking to the correct person.

There are 3 back up questions already created in Omnia:

- 1) What the last 4 digits of you social security number?
- 2) What is your mother's maiden name?
- 3) What is your childhood street name?

The customer can also create a different back up question if they want more security on their account.

When a customer calls in to Customer Care or stops in at a store, the representative needs to complete the following steps:

- 1) Verify the CPNI password.
- 2) If the password is on the Contact Screen it should be transferred to the Profiler Screen.
- 3) If the customer states the correct password you may continue on with what the customer called in about.

- 4) If the customer can not remember what the password was you can ask a back up question to verify who they are

What if the account does not have a CPNI password created?

You can verify the customer with any information you have on the account that maybe only the customer would know.

- 1) Social Security number
- 2) Mailing address
- 3) Last payment to Long Lines

Once you have an answer please create a password and back up question for the customer that will be used from this point going forward.

If the customer can not remember their password what is their choices?

We can call them back at the main number of service we provide. The customer can stop at any Long Lines store and present a photo ID.

Does each person on the account need to have their own password and back up question?

No, all contacts on the account can use the same password, but it the main account holders choice of how they want their account set up. We should have on record the last 4 numbers of each contact name's Social Security number on the account.

Annual 47 C.F.R 64.2013(e) CPNI Certification
EB Docket 06-36

Annual 64.2013(e) CPNI Certification for 2013

Date Filed: January 10, 2014

Name of Company covered by this certification: Long Lines and AT&T

Form 499 Filer ID: 826537 (Long Lines Wireless)

Name of Signatory: Jason Kvidera

Title of Signatory: Financial Manager, Compliance Officer

I, Jason Kvidera, certify that I 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.* I further certify that we continued compliance when AT&T purchased our assets on 12/20/13 through the end of the year on their behalf.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commissions against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPN.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or 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).

The company represents and warrants that the above certification in consistent with 47.C.F.R 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that the 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

A handwritten signature in black ink, appearing to read "Jason Kvidera", with a long horizontal line extending to the right.

January 10, 2014

Dear Federal Communications Commission,

Enclosed is the 2013 CPNI Filing for Long Lines and its affiliate companies. Long Lines is the parent company for the following telecommunication providers:

- Long Lines Wireless (1/1/13 – 12/20/13)
- Long Lines Wireless (purchased by AT&T 12/20/13 -12/31/13)

The above companies were trained and certified by the Long Lines Compliance Officer and follow Long Lines' CPNI rules, regulations, and procedures. We continued this process after AT&T purchased the assets on their behalf.

If you have any questions regarding any of the affiliate companies or need additional information, please feel free to contact me at 712.271.4000.

Sincerely,



Jason Kvidera
Compliance Officer

EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013 OF WILLIAM HAGUE, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY AND CONSUMER MARKETS – INTERNATIONAL, ALLIANCES AND INTEGRATION

Schedule F: Long Lines Wireless Property

In accordance with Section 64.2009(e) of the CPNI rules, AT&T Mobility and Consumer Markets – International, Alliances and Integration (“My Organization”) has adopted procedures that are intended to ensure the compliance of the Long Lines Wireless Property, as defined below, with the FCC’s CPNI rules. This statement summarizes and explains the procedures and explains how these procedures were designed and adopted to ensure compliance with the CPNI rules.

On December 20, 2013, AT&T closed on its acquisition of certain wireless assets of Long Lines Wireless (“Seller”). The acquisition included Seller’s spectrum licenses and network assets in Iowa, Nebraska, Minnesota, South Dakota, and North Dakota, and approximately 10,500 wireless subscribers in Iowa (the “Long Lines Wireless Property”). During December 20, 2013, to December 31, 2013 (the “Time Period”), AT&T Mobility operated the Long Lines Wireless Property under the Long Lines Wireless brand. During the Time Period, AT&T received certain support services from Seller pursuant to a transition services agreement (“TSA”). This Statement addresses AT&T’s operation of the Long Lines Wireless Property during the Time Period. This Statement is based and relies on the following:

- (1) A CPNI Certification filed by Seller with the FCC on January 10, 2014 (“Seller Certification”) which states that during its operation of the Long Lines Wireless Property in 2013, Seller established operating procedures that are adequate to ensure the Long Lines Wireless Property’s compliance with the requirements of the FCC’s CPNI rules procedures (“Legacy Sales Practices”).
- (2) A CPNI Certification filed by Seller with the FCC on January 10, 2014, which states that during the Time Period, Seller continued the Legacy Sales Practices in the provision of services to AT&T under the TSA during the Time Period (the “TSA Certification”).

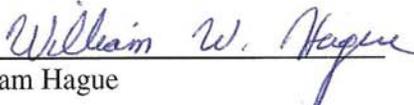
A. Customer CPNI Approvals. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

B. Training and Discipline. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

C. CPNI Complaints and Breaches. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

D. Security and Authentication. During the Time Period, Seller under the TSA continued to follow the Legacy Sales Practices memorialized in the Seller Certification.

Date:


William Hague

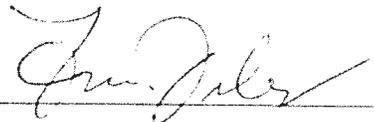
AT&T Inc. CPNI Certification
Calendar Year 2013

Date: 1/23/14

1. I, Frank Jules, President, Global Business Solutions, hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: 

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF Frank Jules, President-Global Business Solutions**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by Global Business Solutions (my organization) ensures compliance with the specific requirements set forth in Subpart U- Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals. To the extent applicable my organization:

1. Follow established and distributed methods and procedures (M&Ps) whereby personnel were not to disclose or permit access to customer's CPNI for out of category services without customer approval or unless such disclosure or access was permitted under FCC rules and personnel were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer's CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).
2. Follow established and distributed M&Ps whereby personnel were required to make a record of a customer's consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).

3. Follow established and distributed M&Ps whereby personnel were prohibited from the use, disclosure or access to a customer's individually identifiable CPNI, except where: (1) the customer granted opt in approval as defined in 47 C.F.R. §64.2003(k); (2) such use or disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).

4. Follow established and distributed M&Ps whereby personnel were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby personnel were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).

5. Follow established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. 47 C.F.R. §64.2008(b) and (c).

6. Follow established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).

7. Follow established M&Ps or implemented systems to clearly establish the status of a customer's CPNI approval prior to the use of CPNI. See 47 C.F.R. §64.2009(a).

B. Training and Discipline: My organization:

1. Requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, my organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any

failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable my organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication. To the extent applicable my organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established procedures for online access to CPNI in a manner consistent with 47 C.F.R. § 64.2010 (c) and (e).
3. Established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).

**AT&T Inc. CPNI Certification
Calendar Year 2013**

Date: 02/10/14

1. I, Glenn Lurie, President – Emerging Enterprises & Partnerships hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: _____



**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF GLENN LURIE, PRESIDENT – EMERGING ENTERPRISES & PARTERSHIPS**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by the Emerging Enterprises & Partnerships organization ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a recurrence.

- A. Customer CPNI Approvals.** To the extent applicable, my organization has:
1. Established processes and controls for employees and dealer agents intended to prohibit the use of, disclosure of, or access to CPNI to market service offerings that are not within a category of service to which the customer already subscribes from AT&T or its affiliates ("out-of-category services") or any other purpose requiring customer approval, unless: (a) such access, use, or disclosure is permitted under the FCC's rules without customer approval, see 47 C.F.R § 64.2005; or (b) the customer granted limited,

one-time use “opt-in approval” as defined in 47 C.F.R § 64.2003(k) for the duration of a call or the duration of a visit. See 47 C.F.R § 64.2007(b) and 47 C.F.R § 64.2008(f).

2. Established processes and controls to maintain a record, for at least one year, of limited, one-time use approval to use a customer’s CPNI to market out-of-category services for the duration of a call or the duration of a visit. See 47 C.F.R. § 64.2007(a)(3).

3. Established and distributed M&Ps and scripts whereby personnel were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer’s right to restrict the use of, disclosure of, and access to that customer’s CPNI. 47 C.F.R. §64.2008(b) and (c).

4. My organization also manages AT&T’s relationship with the following third parties that have access to AT&T customers’ CPNI:

- a. Apple Inc. (“Apple”)
- b. Frontier Communications of America, Inc. (“Frontier”)
- c. Horry Telephone Cooperative, Inc. (“HTC”)
- d. Synchronoss Technologies, Inc. (“STI”)
- e. The Employee Owned Company (“TEOCO”)

Apple, Frontier, and HTC sales personnel have access to CPNI because they sell AT&T wireless services plans. AT&T has provided Apple, Frontier, and HTC with training materials regarding the proper use of CPNI, including the requirement that they obtain consent from customers prior to using CPNI to sell anything other than AT&T wireless services. Apple, Frontier, and HTC have agreed in writing to train their sales representatives on the proper use of CPNI.

STI has access to AT&T customer CPNI as a result of back-office wireless activation support they provide Apple. Certain TEOCO employees have access to CPNI as a result of an analytics tool they created for my organization. STI and TEOCO do not interface with AT&T customers; however, their contracts emphasize the importance of complying with all applicable federal and state laws, specifically including CPNI requirements.

B. Training and Discipline:

1. My organization requires all employees to review and certify to AT&T's Code of Business conduct which includes general information regarding protection of customer records and system access policies. New employees are required to complete this training within 30 days of their start date. AT&T further requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training and provide relevant employees and agents information on CPNI and other privacy related issues through less formal education methods such as employee communications. See 47 C.F.R. §64.2009 (b).
2. AT&T maintains a policy requiring compliance with CPNI rules and advises in the CPNI training and in the Code of Business Conduct that any failure by personnel to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. Security and Authentication. To the extent applicable, my organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).
3. Employed AT&T's established processes and controls to log and process customer-initiated CPNI complaints and breaches (as "breach" is defined in 47 CFR 64.2011(e)) for investigation and resolution for complaint tracking and breach reporting purposes. See 47 C.F.R. §64.2011.

AT&T Inc. CPNI Certification
Calendar Year 2013

Date: Jan. 21, 2014

1. I, Cathy Martine-Dolecki, Executive Vice President, Small Business Solutions & Alternate Channels, hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: Cathy-An Martine-Dolecki

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF Cathy Martine-Dolecki, Executive Vice President-Small Business Solutions &
Alternate Channels**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by Small Business Solutions & Alternate Channels (my organization) ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals. To the extent applicable my organization:

1. Follow established and distributed methods and procedures (M&Ps) whereby personnel were not to disclose or permit access to customer's CPNI for out of category services without customer approval or unless such disclosure or access was permitted under FCC rules and personnel were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer's CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).
2. Follow established and distributed M&Ps whereby personnel were required to make a record of a customer's consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).

3. Follow established and distributed M&Ps whereby personnel were prohibited from the use, disclosure or access to a customer's individually identifiable CPNI, except where: (1) the customer granted opt in approval as defined in 47 C.F.R. §64.2003(k); (2) such use or disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).

4. Follow established and distributed M&Ps whereby personnel were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby personnel were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).

5. Follow established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. 47 C.F.R. §64.2008(b) and (c).

6. Follow established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).

7. Follow established M&Ps or implemented systems to clearly establish the status of a customer's CPNI approval prior to the use of CPNI. See 47 C.F.R. §64.2009(a).

B. Training and Discipline: My organization:

1. Requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, my organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any

failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable my organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication. To the extent applicable my organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established methods and procedures prohibiting the disclosure of call detail over the phone unless the customer provides a password established in a manner consistent with 47 C.F.R. § 64.2010(e)
3. Established procedures for online access to CPNI in a manner consistent with 47 C.F.R. § 64.2010 (c) and (e).
3. Established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).

**AT&T Inc. CPNI Certification
Calendar Year 2013**

Date: 2/12/14

1. I, Stephen A. McGaw, Chief Marketing Officer- AT&T Business Solutions hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: _____



**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF Stephen A. McGaw, Chief Marketing Officer, AT&T Business Solutions**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by the AT&T Business Marketing organization (my organization) ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

1. AT&T Business Marketing has processes in place to protect the access to Customer Proprietary Network Information as defined in 47 C.F.R. § 64.2001 et seq.
2. AT&T Business Marketing has processes and procedures in place designed to obtain customer approval to use, disclose or permit access to CPNI if AT&T intends to use CPNI in circumstances where such approval would be required. As part of the CPNI solicitation process, AT&T advises customers of their right to

restrict use of, disclosure of, and access to CPNI, and provides the customer the requisite notice information required by 47 C.F.R. § 64.2005 and 64.2008.

3. AT&T Business Marketing has established methods and procedures designed to implement customer notifications to comply with the FCC rules to include storage and archiving of notifications for a minimum of one year required by 47 C.F.R. § 64.2008.
4. AT&T Business Marketing has provided adequate training to employees on when they are and are not authorized to use CPNI. AT&T has established a strict Privacy Policy that explains CPNI in detail, and employees adhere to the AT&T Code of Conduct which describes employees' obligation to protect customer information. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. See 47 C.F.R. §64.2009.
5. AT&T Business Marketing has supervisory review processes in place to reasonably ensure compliance with its personnel obtaining supervisory approval of any proposed outbound marketing request for customer approval, and for the maintenance of records related to carrier compliance. See 47 C.F.R. § 64.2009 (d).
6. To the extent applicable, relevant personnel in my organization are aware that:
 - (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system;
 - and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

**AT&T Inc. CPNI Certification
Calendar Year 2013**

Date: 2/26/2014

1. I, Teresa Ostapower, Chief Digital Officer, Digital Experience, Information Technology, hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: 

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF TERESA OSTAPOWER, CHIEF DIGITAL OFFICER- DIGITAL EXPERIENCE,
INFORMATION TECHNOLOGY**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by the Digital Experience Group (my organization) ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

- A. Customer CPNI Approvals.** To the extent applicable my organization has:
1. Established and distributed methods and procedures (M&Ps) whereby personnel were not to disclose or permit access to customer's CPNI for "out of category" services without customer approval or unless such disclosure or access was permitted under FCC rules and personnel were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer's CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).

AT&T Entities

Providing telecommunications (wireless or wireline) and/or interconnected VoIP services

2. Established and distributed M&Ps whereby personnel were required to make a record of a customer's consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).
3. Established and distributed M&Ps whereby personnel were prohibited from the use, disclosure or access to a customer's individually identifiable CPNI, except where: (1) the customer granted "opt in approval" as defined in 47 C.F.R. §64.2003(k); (2) such use or disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).
4. Established and distributed M&Ps whereby personnel were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby personnel were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).
5. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. 47 C.F.R. §64.2008(b) and (c).
6. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).
7. Established M&Ps or implemented systems to clearly establish the status of a customer's CPNI approval prior to the use of CPNI. See 47 C.F.R. §64.2009(a).

B. Training and Discipline: My organization requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, my organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the

AT&T Entities

Providing telecommunications (wireless or wireline) and/or interconnected VoIP services

Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

1. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable my organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication. To the extent applicable my organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established methods and procedures prohibiting the disclosure of call detail over the phone unless the customer provides a password established in a manner consistent with 47 C.F.R. § 64.2010(e)
3. Established procedures for online access to CPNI in a manner consistent with 47 C.F.R. § 64.2010 (c) and (e).¹
4. Established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).

¹ During process reviews in 2013, AT&T noted a defect in the backup authentication procedures for business wireless customer administrators and account managers. AT&T has since corrected this problem and is not aware of any complaints or other evidence indicating that any improper disclosure of CPNI occurred as a result of this issue.

**AT&T Inc. CPNI Certification
Calendar Year 2013**

Date: 2/7/14

1. I, Kevin Peters, Executive Vice President of AT&T Global Customer Service hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: _____

A handwritten signature in black ink, appearing to read "Kevin Peters", is written over a horizontal line. The signature is stylized and includes a vertical line extending downwards from the end of the signature.

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
OF Kevin Peters, Executive Vice President of AT&T Global Customer Service**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by AT&T Global Customer Service (my organization) ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals. To the extent applicable my organization has:

1. Established and distributed methods and procedures (M&Ps) whereby personnel were not to disclose or permit access to customer's CPNI for "out of category" services without customer approval or unless such disclosure or access was permitted under FCC rules and personnel were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer's CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).

2. Established and distributed M&Ps whereby personnel were required to make a record of a customer's consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).
3. Established and distributed M&Ps whereby personnel were prohibited from the use, disclosure or access to a customer's individually identifiable CPNI, except where: (1) the customer granted "opt in approval" as defined in 47 C.F.R. §64.2003(k); (2) such use or disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).
4. Established and distributed M&Ps whereby personnel were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby personnel were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).
5. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. 47 C.F.R. §64.2008(b) and (c).
6. Established and distributed M&Ps or scripts whereby personnel were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).

B. Training and Discipline: My organization:

1. Requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, my organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable my organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication. To the extent applicable my organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established methods and procedures prohibiting the disclosure of call detail over the phone unless the customer provides a password established in a manner consistent with 47 C.F.R. § 64.2010(e)
3. Established procedures for online access to CPNI in a manner consistent with 47 C.F.R. § 64.2010 (c) and (e).
4. Established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).

**AT&T Inc. CPNI Certification
Calendar Year 2013**

Date: 7 February 2013

1. I, Paul Roth, President – AT&T Mobility Retail Sales and Service hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature:  _____

**EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013
Of Paul Roth, President – AT&T Mobility Retail Sales and Service**

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by the AT&T Mobility Retail Sales and Service (My Organization) ensures compliance with the specific requirements set forth in 47 C.F.R. Part 64 Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in My Organization, or (ii) developed by other organizations, in which case My Organization operates in compliance with such applicable processes and procedures. My Organization has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, My Organization investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals. To the extent applicable My Organization has:

1. Established processes and controls intended to prohibit the use of, disclosure of, or access to CPNI to market service offerings that are not within a category of service to which the customer already subscribes from AT&T or its affiliates ("out-of-category services") or any other purpose requiring customer approval, unless: (a) such access, use, or disclosure is permitted under the FCC's rules without customer approval. See 47 C.F.R. § 64.2005; or (b) the customer granted limited, one-time use "opt-in approval" as defined in 47 C.F.R. § 64.2003(k) for the duration of a call or the duration of a visit. See 47 C.F.R. § 64.2007(b) and 47 C.F.R. § 64.2008(f).

2. Established processes and controls to maintain a record, for at least one year, of limited, one-time use approval to use a customer's CPNI to market out-of-category services for the duration of a call or the duration of a visit. See 47 C.F.R. § 64.2007(a)(3).
3. Established processes and controls requiring oral notification of the customer's right to restrict use of, disclosure of, and access to that customer's CPNI consistent with 47 C.F.R. § 64.2008(a)(1) and to provide the customer the requisite notice information required by 47 C.F.R. § 64.2008(c) prior to any solicitation for limited, one-time use approval to use CPNI to market "out of category" services. See 47 C.F.R. § 64.2008(f).
4. My organization has reinforced the requirement AT&T imposes on agents that sell AT&T services to include CPNI disclosures in their order flow.

B. Training and Discipline: My organization:

1. Requires all personnel who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, my organization periodically provides such personnel information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner and all AT&T employees are required to review the Code of Business Conduct, that contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).
2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: To the extent applicable my organization has apprised relevant personnel that: (a) they are required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system; and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Sales and Marketing Campaigns. All Sales and Marketing Campaigns in which My Organization engages are governed by processes and procedures whereby such activities are reviewed and receive the requisite supervisory approval and in connection with which the requisite records are maintained for a one year period. See 47 C.F.R. § 64.2005 and 64.2008

E. Security and Authentication. To the extent applicable my organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established a policy that prohibits access to or disclosure of CPNI except to customers and authorized users who first provide a valid photo ID matching their name on the account. See 47 C.F.R. § 64.2010(d).
3. Established processes and controls to authenticate a customer or authorized user without the use of readily available biographical information or account information in order to establish a password that grants access to CPNI. See 47 CFR 64.2010(e).
4. Employed AT&T's established processes and controls to log and process customer-initiated CPNI complaints and breaches (as "breach" is defined in 47 CFR 64.2011(e)) for investigation and resolution and for complaint tracking and breach reporting purposes. See 47 CFR § 64.2011.

AT&T Inc. CPNI Certification

Calendar Year 2013

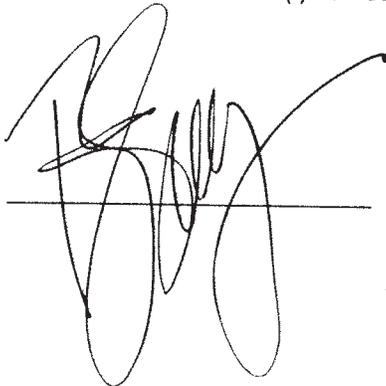
Date: 2/10/14

1. I, Brian Shay, Executive Vice President, AT&T Mobility Customer Service ("Responsible Business Unit") hereby certify, based upon my own personal knowledge or the personal knowledge of AT&T subject matter experts upon whom I have reasonably relied in making this certification, that the statements and information contained herein are accurate and complete. In making this certification, I have made a reasonable and diligent inquiry into the facts, including discussions with AT&T subject matter experts and a review of all necessary supporting documentation, either conducted by myself or by persons acting under my direction and control.

2. In accordance with the requirements of 47 C.F.R. §64.2009(e), I certify that, as of December 31, 2013, the Responsible Business Unit(s) for which I am accountable has established safeguards and operating procedures adequate to ensure compliance with the requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules, 47 C.F.R. § 64.2001 et. seq. (the "FCC's CPNI rules").

3. I further certify that I am not aware of any known instances of non-compliance with the above requirements that have not been (i) corrected; or (ii) otherwise disclosed in this certificate.

Signature: _____

A handwritten signature in black ink, appearing to be "Brian Shay", written over a horizontal line. The signature is stylized and cursive.

EXPLANATORY STATEMENT OF CPNI COMPLIANCE FOR 2013

OF BRIAN SHAY, EXECUTIVE VICE PRESIDENT, AT&T MOBILITY CUSTOMER SERVICE

In accordance with Section 64.2009(e) of the CPNI rules, I am providing the following explanation of how the operating procedures established by the AT&T Mobility Customer Service organization (my organization) ensures compliance with the specific requirements set forth in Subpart U-Customer Proprietary Network Information of the FCC's rules. This statement summarizes and explains the procedures and explains how these procedures were designed to ensure compliance with the CPNI rules. The described processes and procedures have either been (i) developed and implemented in my organization, or (ii) developed by other organizations, in which case my organization operates in compliance with such applicable processes and procedures. AT&T has established corrective processes to detect and cure potential deficiencies in the implementation and maintenance of its CPNI operating procedures. To the extent AT&T discovers or is made aware of an error, AT&T investigates the cause of the error, fixes the error, and, if necessary, updates its methods and procedures and provides additional training to prevent a reoccurrence.

A. Customer CPNI Approvals. To the extent applicable, my organization has:

1. Established and distributed methods and procedures (M&Ps) whereby AT&T employees, agents, and representatives were not to disclose or permit access to customer's CPNI for "out of category" services without customer approval or unless such disclosure or access was permitted under FCC rules and AT&T employees, agents, and representatives were apprised that any approval or disapproval by a customer of the use, disclosure or access to the customer's CPNI must remain in effect until revocation or limitation of such approval or disapproval. See 47 C.F.R. §64.2005(a) and (b), and 47 C.F.R. §64.2007(a)(2).
2. Established and distributed M&Ps whereby AT&T employees, agents, and representatives were required to make a record of a customer's consent to the use of CPNI information. Such records are maintained for at least one year. See 47 C.F.R. §64.2007(a)(3).
3. Established and distributed M&Ps whereby AT&T employees, agents, and representatives were prohibited from the use, disclosure or access to a customer's individually identifiable CPNI, except where: (1) the customer granted "opt in approval" as defined in 47 C.F.R. §64.2003(k); (2) such use or disclosure was permissible under 47 C.F.R. §64.2005; (3) such use or disclosure was otherwise permissible under section 222 of the Telecommunications Act of 1934, as amended. See 47 C.F.R. §64.2007(b).

4. Established and distributed M&Ps whereby AT&T employees, agents, and representatives were required, prior to any solicitation for customer approval to use, disclose, or permit access to the customer's CPNI, to notify the customer of the customer's right to restrict use, disclosure and access to CPNI. See 47 C.F.R. §64.2008(a)(1). Also, established and distributed M&Ps whereby AT&T employees, agents, and representatives were required to make a record of customer's consent to the use of CPNI information in compliance with 47 C.F.R. §64.2007(a)(3) and 47 C.F.R. §64.2008(a)(1).

5. Established and distributed M&Ps or scripts whereby AT&T employees, agents, and representatives were required, prior to any oral solicitation for customer approval, to notify the customer on an individual basis of the customer's right to restrict the use of, disclosure of, and access to that customer's CPNI. 47 C.F.R. §64.2008(b) and (c).

6. Maintained an IVR and toll free number with voice mail whereby customers, at no additional cost, could avail themselves of an "opt-out" method. The IVR and voice mail were available 24 hours a day, seven days a week. See 47 C.F.R. §64.2008(d)(3)(v).

7. Established and distributed M&Ps or scripts whereby AT&T employees, agents, and representatives were required, prior to any oral solicitation for limited, one time use of a customer's CPNI for duration of the call, to provide the customer with the required notifications as set forth in 47 C.F.R. §64.2008(f).

8. Established M&Ps or implemented systems to clearly establish the status of a customer's CPNI approval prior to the use of CPNI. See 47 C.F.R. §64.2009(a).

B. Training and Discipline: My organization:

1. Requires all AT&T employees, agents, and representatives who have access to customer data or who have outbound marketing responsibilities to complete specific CPNI training. In addition, my organization periodically provides such AT&T employees, agents, and representatives information on CPNI and other privacy related issues through less formal education methods such as employee communications, refresher training, and meetings. Further, vendors have contractual obligations to follow CPNI regulations and to conduct themselves in an ethical manner, and all AT&T employees are required to review the Code of Business Conduct, which contains CPNI information, on an annual basis. See 47 C.F.R. §64.2009 (b).

2. AT&T maintains a policy requiring compliance with CPNI rules. Any failure by employees to comply with CPNI rules is subject to disciplinary action up to and including termination of employment, depending on the severity of the non-compliance. Similarly, any failure by vendor employees to comply with CPNI rules subjects them to removal from AT&T's program depending on the severity of the non-compliance. See 47 C.F.R. §64.2009 (b).

C. CPNI Complaints and Breaches: My organization has established and distributed M&Ps whereby AT&T employees, agents, and representatives are: (a) required to make a record of any customer complaint regarding unauthorized access to, disclosure or release of CPNI through a tracking system;

and (b) they are required to refer complaints to the appropriate business organization if the complaint involves fraud or identity theft. See 47 C.F.R. §64.2009 (e).

D. Security and Authentication. My organization has:

1. Established account access policies that outline what information is required to properly authenticate a customer or an authorized user before release of CPNI for all applicable points of access. See C.F.R. § 64.2010(a).
2. Established methods and procedures prohibiting the disclosure of call detail over the phone unless the customer provides a password established in a manner consistent with 47 C.F.R. § 64.2010(e).
3. Established procedures that notify customers immediately when there has been a change to the account as contemplated by 47 C.F.R. §64.2010 (f).
4. Where appropriate, created and maintained desktop tools to support the M&Ps identified herein.

ATTACHMENT A
AT&T CY2013 Annual CPNI Certifications

Page 1 of 2

AT&T Entities

Providing telecommunications (wireless or wireline) and/or interconnected VoIP services

Name of FCC-Regulated Business	FCC Registration Number
Acadiana Cellular General Partnership	0001837814
Aio Wireless LLC	0022720445
Alascom, Inc.	0001572676
Ameritech Services, Inc.	0007586290
AT&T Communications Of Indiana, GP	0012838421
AT&T Communications Of New York, Inc.	0012838462
AT&T Communications Of Texas, LLC	0016657918
AT&T Communications Of Virginia, LLC	0012838546
AT&T Corp.	0005937974
AT&T Management Services, L.P.	0002534451
AT&T Mobility LLC	0004979233
AT&T Mobility Of Galveston LLC	0016658122
AT&T Mobility Puerto Rico Inc.	0003473709
AT&T Mobility Spectrum LLC	0014980726
AT&T Mobility USVI Inc.	0004499034
AT&T Mobility Wireless Operations Holdings Inc.	0020078887
AT&T Of Puerto Rico, Inc.	0001731462
AT&T Of The Virgin Islands, Inc.	0003464344
AT&T Services, Inc.	0008644056
AWS Wireless Inc.	0015022023
Bellsouth Long Distance, Inc.	0003733318
Bellsouth Telecommunications, LLC	0020882668
Bristol Bay Cellular Partnership	0001568898
Centennial Communications Corp.	0009631136
Chattanooga MSA Limited Partnership	0001842723
Cingular Wireless Of Texas RSA #11 Limited Partnership	0003294048
Cingular Wireless Of Texas RSA #16 Limited Partnership	0003294006
Decatur RSA Limited Partnership	0004588455
Elkhart Cellular Telephone Company	0012927109
Florida RSA No. 2B (Indian River) Limited Partnership	0001837566
Georgia R.S.A. #8 Partnership	0001838069
Georgia RSA No. 3 Limited Partnership	0001836998
Houma-Thibodaux Cellular Partnership	0004547931
Illinois Bell Telephone Company	0002860856
Indiana Bell Telephone Company, Incorporated	0002904654
Lafayette MSA Limited Partnership	0001682509
Louisiana RSA No. 7 Cellular General Partnership	0001837798
Louisiana RSA No. 8 Limited Partnership	0001837830
Lubbock SMSA Limited Partnership	0001650787
Madison SMSA Limited Partnership	0002842060

ATTACHMENT A
AT&T CY2013 Annual CPNI Certifications

Page 2 of 2

AT&T Entities

Providing telecommunications (wireless or wireline) and/or interconnected VoIP services

Name of FCC-Regulated Business	FCC Registration Number
McAllen-Edinburg-Mission SMSA Limited Partnership	0001658467
Michigan Bell Telephone Company	0002776771
Milwaukee SMSA Limited Partnership	0002846293
Missouri RSA 11/12 Limited Partnership	0001658418
Missouri RSA 8 Limited Partnership	0001658442
Missouri RSA 9B1 Limited Partnership	0001658426
NC Tide Acquisition Company LLC	0022291900
NE-1 Acquisition Company LLC	0017686395
Nevada Bell Telephone Company	0001552173
New Cingular Wireless PCS, LLC	0003291192
Northeastern Georgia RSA Limited Partnership	0001837152
Ohio RSA #3 Limited Partnership	0002151413
Ohio RSA 2 Limited Partnership	0002837094
Ohio RSA 5 Limited Partnership	0002837110
Ohio RSA 6 Limited Partnership	0002837136
Oklahoma City SMSA Limited Partnership	0001658392
Oklahoma Independent RSA 7 Partnership	0010698884
Oklahoma RSA 3 Limited Partnership	0001658376
Oklahoma RSA 9 Limited Partnership	0001658368
Orlando SMSA Limited Partnership	0001843036
Pacific Bell Telephone Company	0001551530
Red WL Corp.	0002623601
Santa Barbara Cellular Systems, Ltd.	0004312898
SBC Long Distance, LLC	0003763497
SNET America, Inc.	0003737707
SNET Diversified Group, Inc.	0007586423
Southwestern Bell Telephone Company	0016627473
TC Systems, Inc.	0012833513
TCG South Florida	0014533079
Teleport Communications America, LLC	0022315121
Teleport Communications Atlanta, Inc.	0014533178
Teleport Communications New York	0014533301
Texas RSA 18 Limited Partnership	0001666072
Texas RSA 19 Limited Partnership	0001666056
Texas RSA 20B1 Limited Partnership	0001665058
Texas RSA 6 Limited Partnership	0001665991
Texas RSA 7B1 Limited Partnership	0001666007
Texas RSA 9B1 Limited Partnership	0001666023
Texas RSA No. 2 Limited Partnership	0004550547
The Ohio Bell Telephone Company	0002946986
The Southern New England Telephone Company	0003576931

AT&T Entities

Providing telecommunications (wireless or wireline) and/or interconnected VoIP services

Name of FCC-Regulated Business	FCC Registration Number
Tide Mobility LLC	0022415855
Topeka SMSA Limited Partnership	0001658632
WCS Wireless License Subsidiary, LLC	0009850488
Wisconsin Bell, Inc.	0002716561

ATTACHMENT B
AT&T CY2013 Annual CPNI Certifications

**Summary of Customer Complaints and
Actions Taken Against Data Brokers**

Summary of Customer Complaints

As required by 47 C.F.R. §64.2009(e), following is a summary of customer complaints concerning the unauthorized release of Customer Proprietary Network Information (CPNI) received by AT&T Inc. from January 1, 2013 to December 31, 2013:

CPNI COMPLAINT CATEGORY	Number of Customer Complaints 2013
Accessed online by an unauthorized third party (i.e. not by an AT&T employee/agent)	103
Disclosed to an unauthorized third party (i.e. not to an AT&T employee/agent)	58
Unauthorized access or disclosure by an AT&T employee or AT&T agent	534
Grand Total	695

Summary of Actions Taken Against Data Brokers

The company 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.