

Tamara Preiss  
Vice President  
Federal Regulatory Affairs



September 28, 2010

1300 I Street, NW, Suite 400 West  
Washington, DC 20005

Phone 202 515-2540  
Fax 202 336-7922  
tamara.preiss@verizon.com

**VIA ECFS**

Marlene H. Dortch  
Office of the Secretary  
Federal Communications Commission  
445 12<sup>th</sup> St., SW  
Suite TW-A235  
Washington, DC 20554

**Re: Annual Section 64.2009(e) CPNI Certification, EB Docket No. 06-36**

Dear Ms. Dortch:

As a result of a merger that was consummated on January 9, 2009, Alltel Communications, LLC ("Alltel") became a wholly-owned subsidiary of Cellco Partnership d/b/a Verizon Wireless. As a condition of approval of this merger, the Department of Justice and the Federal Communications Commission required Verizon Wireless to divest certain markets, and a Management Trustee was appointed to manage the divested markets until they were sold. Sale of the remaining divested markets to AT&T was completed on June 22, 2010.

Pursuant to Section 64.2009(e) of the Commission's rules, 47 C.F.R. § 64.2009(e), the Verizon /Alltel Management Trust hereby files its annual certification of compliance with the Commission's customer proprietary network information (CPNI) rules for the period January 1, 2010 through June 21, 2010, with respect to the divested markets managed by the Management Trustee.

Please contact the undersigned should you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Tamara Preiss".

Attachments

cc: Best Copy and Printing

**ANNUAL SECTION 64.2009(e) CPNI CERTIFICATION**  
**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification

Date filed: September 28, 2010

Period covered by this certification: January 1, 2010 through June 21, 2010 ("Relevant Period")

Name of company covered by this certification: Alltel Communications, LLC, with respect to the divested markets which were managed by the Management Trust established in connection with the merger of Cellco Partnership d/b/a Verizon Wireless and Alltel Corporation and its subsidiaries, including Alltel Communications, LLC

Name and title of signatory: Barbara P. Bonds, former Trust Counsel

I, Barbara P. Bonds, was the Trust Counsel for the Verizon/Alltel Management Trust, which was established January 9, 2009, in connection with the merger of Cellco Partnership d/b/a Verizon Wireless with Alltel Corporation and its subsidiaries, including Alltel Communications, LLC . As a condition of approval of this merger, the Department of Justice and the FCC required Verizon Wireless to divest certain markets, and a Management Trustee was appointed to manage the divested markets until they were sold. The sale of remaining divested markets to AT&T was closed June 22, 2010. I served in the capacity of Trust Counsel from January 9, 2009, through June 21, 2010. As former Trust Counsel, I hereby certify on behalf of the divested markets managed by the Verizon/Alltel Management Trust, referred to herein as "Alltel," that I have personal knowledge that Alltel had established operating procedures, as described in sections D 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 were adequate to ensure compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended. To the extent that the attached Statement refers to activities performed by employees of Verizon Wireless that were designated to provide shared support and serve as consultants to the Management Trust during the Relevant Period, this will be addressed in the annual Section 64.2009(e) CPNI Certification to be filed by Cellco Partnership d/b/a Verizon Wireless.

Attached to this certification is an accompanying statement explaining how Alltel's procedures ensured that Alltel was 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 concerning the unauthorized release of CPNI.

  
Barbara P. Bonds  
Former Trust Counsel,  
Verizon/Alltel Management Trust

*August 27, 2010*

**STATEMENT OF OPERATING PROCEDURES IMPLEMENTING  
47 C.F.R. SUBPART U GOVERNING USE OF  
CUSTOMER PROPRIETARY NETWORK INFORMATION  
FOR THE PERIOD JANUARY 1, 2010 TO JUNE 21, 2010**

On January 9, 2009, Cellco Partnership d/b/a Verizon Wireless acquired Alltel Corporation and its subsidiaries, including Alltel Communications, LLC (“Alltel”). In connection with the approval of this merger, the Department of Justice and the FCC required Verizon Wireless to divest certain markets. A Management Trustee was appointed to manage the divested markets until they were sold. The divested markets were managed and operated in a Management Trust as a separate business from Verizon Wireless. For the duration of the Management Trust, the divested markets were operated under the Alltel brand and Alltel’s prior policies remained in effect. The sale of the remaining divested markets to AT&T was closed June 22, 2010. This Statement of Operating Procedures was in effect from January 1, 2010, through June 21, 2010 (the “Relevant Period”), which was the portion of 2010 during which the Management Trust was in effect. References to “Alltel” herein refer only to the divested markets managed by the Management Trust. The following statement submitted on behalf of the divested Alltel markets managed by the Management Trust explains how the operating procedures of Alltel 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. The Management Trust did not have corporate officers; the persons signing the annual Section 64.2009(e) certification on behalf of the Management Trust were senior leaders of the Trust comparable to corporate officers.

**A. CPNI Use and Customer Approval**

In accordance with 47 CFR 64.2005(a), Alltel 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 relevant time period, Alltel offered CMRS and information services. Consistent with 47 CFR 64.2005(b), Alltel did not use, disclose, or permit access to CPNI to market telecommunication service offerings outside the category of service to which the customer subscribed. Alltel used CPNI derived from the provision of CMRS for the provision of CPE and information services. Alltel did not solicit customer consent to use CPNI in a manner that was beyond its then existing service relationship and Alltel did not consider its customers 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 customers’ individually identifiable CPNI for marketing communications-related services to such customers did not apply to Alltel's operational use of CPNI during the relevant period. Alltel maintained a CPNI Marketing Policy which defined how CPNI could be used to market and provide services to Alltel customers. In accordance with that policy, Alltel required that CPNI be used only for the purposes identified herein and as otherwise permitted.

**B. Sales and Marketing Campaigns**

Pursuant to 47 CFR 64.2009, Alltel 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 Alltel in accordance with 47 CFR 64.2005(a). Alltel did not engage in cross service marketing campaigns. In addition and consistent with 47 CFR 64.2009(d), Alltel had a supervisory review process to evaluate the proposed use of CPNI in outbound marketing campaigns. Alltel 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 at minimum Director level employees.

Consistent with 47 CFR 64.2009(c), Alltel maintained records of the campaigns which used CPNI that were conducted by authorized personnel. Alltel's Privacy Office, which included certain Verizon Wireless employees who were designated to provide shared support and serve as consultants to the Management Trust, conducted quarterly reviews of such campaign records to verify compliance with CPNI rules and Alltel policies. 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. The results of the quarterly reviews were also analyzed by the Privacy Office and the Trust marketing staff to verify compliance with CPNI rules.

### **C. Training and Disciplinary Process**

Alltel employees authorized to conduct marketing campaigns were trained to keep customer data strictly confidential. During the prior reporting period, Alltel's Privacy Office conducted periodic CPNI education for personnel who were authorized to conduct campaigns as required by 47 CFR 64.2009(b). Specifically, such personnel were instructed as to the proper access and use of CPNI. Each person authorized to conduct a marketing campaign utilizing CPNI received this training.

Alltel's CPNI Marketing Policy expressly established a disciplinary process applicable to employees in the event it was determined that such policy had been violated. A violation of such policy would subject the employee to disciplinary action, up to and including termination.

### **BPB D. Security Governance**

Alltel maintained an "Enterprise Information Security Program" (EISP) designed to protect all of the data collected, generated, created, stored, managed, transmitted or otherwise handled by Alltel.

### **BPB E. Billing Records, Network Records, and Information**

Alltel 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.

Internal governance processes dictated that newly created applications and

significant changes to existing applications that processed or stored customer data must be formally reviewed and analyzed by appropriate security and privacy teams. Alltel's corporate security team reviewed new applications and enhancements for compliance with existing security and privacy policies, which included requirements for access and authentication controls.

**BPB 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 Alltel's Privacy Office and the shared services Internal Audit Department during the prior reporting period.

**BPB G. Safeguards on the Disclosure of CPNI**

**(1) Safeguarding CPNI**

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

Alltel 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. Alltel 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. Initial access to a number of applications was controlled via an internal application that used role-based logic and employee job requirements, as defined by the designated business owners, to limit access based on job function.

Alltel's privacy statement described how Alltel used, maintained and protected customer information, including CPNI. During the relevant time period this statement was available to all customers at [www.alltel.com](http://www.alltel.com) by clicking on 'Privacy Statement' at the bottom of Alltel's home page. In addition, Alltel'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, Alltel customer service representatives were prohibited from disclosing call detail (as defined in 47 CFR 64.2003(d)) over the telephone. 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, Alltel would mail a copy of call detail 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, Alltel did not mail the requested call detail. Instead, Alltel advised such customers to utilize online or in-store access. Alltel policy did not permit faxing of call detail.

### **(3) Online Access to CPNI**

Alltel maintained an online account retrieval system called "My Account" whereby Alltel customers could register their account and subsequently login to access their account information and CPNI only after providing a valid password. Prior to the relevant time period, Alltel had established operating procedures adequate to ensure compliance with the CPNI rules relating to online access to CPNI, including a requirement that all 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.

Alltel 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 Alltel their account number and mobile number. The post paid 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. Post paid 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, post paid customers were required to utilize their user identification and password for online access to CPNI.

My Account registration for Alltel business customers required two data elements in addition to the My Account registration process for post paid consumers. Business customers were required to provide their business' tax identification number to Alltel and to create a personal identification number (PIN) after they entered their user identification and password. For on-line access to CPNI after the registration for a business account was complete, users were required to submit their user identification, password and PIN.

Alltel prepaid customers registered for online access to CPNI in the same manner as described above. Prepaid 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, prepaid customers were required to utilize their user identification and password for online access to CPNI.

Additionally, Alltel 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 or Forgotten Passwords.**

Alltel made available a backup authentication method for customers who had forgotten their My Account password. This backup authentication method did not prompt the customer for readily available biographical or account information. If the 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 Alltel prior to establishing a new password.

### **(5) Notification of Account Changes**

Alltel 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. Alltel did not reveal the changed information.

### **(6) In-Store Access to CPNI**

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

### *BPB* **H. Notification of CPNI Security Breaches**

Alltel's existing processes ensured compliance with the CPNI rules. Periodic meetings were conducted among Alltel's corporate security team and Trust Legal staff to consider internal investigations involving potential CPNI breaches. Alltel reported confirmed CPNI breaches and notified customers in accordance with the CPNI breach notification rules.

### *BPB* **I. Summary of Customer Complaints Regarding the Unauthorized Release of CPNI**

During the relevant period Alltel's physical security group completed 16 data breach series investigations; of these, 13 originated from complaints from customers regarding the unauthorized release of CPNI. Alltel's corporate security group investigated these complaints and 12 of them did not appear to result in improper access to or unauthorized release of CPNI. There were 4 instances of apparent improper access and improper disclosure by employees to unauthorized individuals.

### *BPB* **J. Action Taken Against Data Brokers**

During the Relevant Period, Alltel did not initiate any actions against data brokers.

**ANNUAL SECTION 64.2009(e) CPNI CERTIFICATION**  
**EB Docket 06-36**

Annual 64.2009(e) CPNI Certification

Date filed: September 28, 2010

Period covered by this certification: January 1, 2010 through June 21, 2010 ("Relevant Period")

Name of company covered by this certification: Alltel Communications, LLC, with respect to the divested markets which were managed by the Management Trust established in connection with the merger of Cellco Partnership d/b/a Verizon Wireless and Alltel Corporation and its subsidiaries, including Alltel Communications, LLC

Name and Title of Signatory: Rebecca Hauman, former Director of Strategic Marketing

I, Rebecca Hauman, was Director of Strategic Marketing for the Verizon/Alltel Management Trust, which was established January 9, 2009, in connection with the merger of Cellco Partnership d/b/a Verizon Wireless with Alltel Corporation and its subsidiaries, including Alltel Communications, LLC. As a condition of approval of this merger, the Department of Justice and the FCC required Verizon Wireless to divest certain markets, and a Management Trustee was appointed to manage the divested markets until they were sold. The sale of remaining divested markets to AT&T closed June 22, 2010. I served in the capacity of Director of Strategic Marketing from January 9, 2009, through June 21, 2010. As the former Director of Strategic Marketing, I hereby certify on behalf of the divested markets managed by the Verizon/Alltel Management Trust, referred to herein as "Alltel," that I have personal knowledge that Alltel had established operating procedures, as described in sections A through C of the attached STATEMENT OF OPERATING PROCEDURES IMPLEMENTING 47 C.F.R. SUBPART U GOVERNING USE OF CUSTOMER PROPRIETARY NETWORK INFORMATION ("Statement"), that were adequate to ensure compliance with the rules of the Federal Communications Commission set forth in 47 C.F.R. Subpart U, implementing Section 222 of the Communications Act of 1934, as amended. To the extent that the attached Statement refers to activities performed by employees of Verizon Wireless that were designated to provide shared support and serve as consultants to the Management Trust during the Relevant Period, this will be addressed in the annual Section 64.2009(e) CPNI Certification to be filed by Cellco Partnership d/b/a Verizon Wireless.

Attached to this certification is an accompanying statement explaining how Alltel's procedures ensured that Alltel was 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 concerning the unauthorized release of CPNI.



Rebecca Hauman  
Former Director of Strategic Marketing  
Verizon/Alltel Management Trust

August 27, 2010

**STATEMENT OF OPERATING PROCEDURES IMPLEMENTING  
47 C.F.R. SUBPART U GOVERNING USE OF  
CUSTOMER PROPRIETARY NETWORK INFORMATION  
FOR THE PERIOD JANUARY 1, 2010 TO JUNE 21, 2010**

On January 9, 2009, Cellco Partnership d/b/a Verizon Wireless acquired Alltel Corporation and its subsidiaries, including Alltel Communications, LLC ("Alltel"). In connection with the approval of this merger, the Department of Justice and the FCC required Verizon Wireless to divest certain markets. A Management Trustee was appointed to manage the divested markets until they were sold. The divested markets were managed and operated in a Management Trust as a separate business from Verizon Wireless. For the duration of the Management Trust, the divested markets were operated under the Alltel brand and Alltel's prior policies remained in effect. The sale of the remaining divested markets to AT&T was closed June 22, 2010. This Statement of Operating Procedures was in effect from January 1, 2010, through June 21, 2010 (the "Relevant Period"), which was the portion of 2010 during which the Management Trust was in effect. References to "Alltel" herein refer only to the divested markets managed by the Management Trust. The following statement submitted on behalf of the divested Alltel markets managed by the Management Trust explains how the operating procedures of Alltel 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. The Management Trust did not have corporate officers; the persons signing the annual Section 64.2009(e) certification on behalf of the Management Trust were senior leaders of the Trust comparable to corporate officers.

*reh* **A. CPNI Use and Customer Approval**

In accordance with 47 CFR 64.2005(a), Alltel 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 relevant time period, Alltel offered CMRS and information services. Consistent with 47 CFR 64.2005(b), Alltel did not use, disclose, or permit access to CPNI to market telecommunication service offerings outside the category of service to which the customer subscribed. Alltel used CPNI derived from the provision of CMRS for the provision of CPE and information services. Alltel did not solicit customer consent to use CPNI in a manner that was beyond its then existing service relationship and Alltel did not consider its customers 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 customers' individually identifiable CPNI for marketing communications-related services to such customers did not apply to Alltel's operational use of CPNI during the relevant period. Alltel maintained a CPNI Marketing Policy which defined how CPNI could be used to market and provide services to Alltel customers. In accordance with that policy, Alltel required that CPNI be used only for the purposes identified herein and as otherwise permitted.

*reh* **B. Sales and Marketing Campaigns**

*reh*

Pursuant to 47 CFR 64.2009, Alltel 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 Alltel in accordance with 47 CFR 64.2005(a). Alltel did not engage in cross service marketing campaigns. In addition and consistent with 47 CFR 64.2009(d), Alltel had a supervisory review process to evaluate the proposed use of CPNI in outbound marketing campaigns. Alltel 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 at minimum Director level employees.

Consistent with 47 CFR 64.2009(c), Alltel maintained records of the campaigns which used CPNI that were conducted by authorized personnel. Alltel's Privacy Office, which included certain Verizon Wireless employees who were designated to provide shared support and serve as consultants to the Management Trust, conducted quarterly reviews of such campaign records to verify compliance with CPNI rules and Alltel policies. 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. The results of the quarterly reviews were also analyzed by the Privacy Office and the Trust marketing staff to verify compliance with CPNI rules.

**C. Training and Disciplinary Process**

*reh*

Alltel employees authorized to conduct marketing campaigns were trained to keep customer data strictly confidential. During the prior reporting period, Alltel's Privacy Office conducted periodic CPNI education for personnel who were authorized to conduct campaigns as required by 47 CFR 64.2009(b). Specifically, such personnel were instructed as to the proper access and use of CPNI. Each person authorized to conduct a marketing campaign utilizing CPNI received this training.

Alltel's CPNI Marketing Policy expressly established a disciplinary process applicable to employees in the event it was determined that such policy had been violated. A violation of such policy would subject the employee to disciplinary action, up to and including termination.

**D. Security Governance**

Alltel maintained an "Enterprise Information Security Program" (EISP) designed to protect all of the data collected, generated, created, stored, managed, transmitted or otherwise handled by Alltel.

**E. Billing Records, Network Records, and Information**

Alltel 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.

Internal governance processes dictated that newly created applications and

significant changes to existing applications that processed or stored customer data must be formally reviewed and analyzed by appropriate security and privacy teams. Alltel's corporate security team reviewed new applications and enhancements for compliance with existing security and privacy policies, 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 Alltel's Privacy Office and the shared services Internal Audit Department during the prior reporting period.

#### **G. Safeguards on the Disclosure of CPNI**

##### **(1) Safeguarding CPNI**

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

Alltel 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. Alltel 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. Initial access to a number of applications was controlled via an internal application that used role-based logic and employee job requirements, as defined by the designated business owners, to limit access based on job function.

Alltel's privacy statement described how Alltel used, maintained and protected customer information, including CPNI. During the relevant time period this statement was available to all customers at [www.alltel.com](http://www.alltel.com) by clicking on 'Privacy Statement' at the bottom of Alltel's home page. In addition, Alltel'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, Alltel customer service representatives were prohibited from disclosing call detail (as defined in 47 CFR 64.2003(d)) over the telephone. 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, Alltel would mail a copy of call detail 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, Alltel did not mail the requested call detail. Instead, Alltel advised such customers to utilize online or in-store access. Alltel policy did not permit faxing of call detail.

### **(3) Online Access to CPNI**

Alltel maintained an online account retrieval system called "My Account" whereby Alltel customers could register their account and subsequently login to access their account information and CPNI only after providing a valid password. Prior to the relevant time period, Alltel had established operating procedures adequate to ensure compliance with the CPNI rules relating to online access to CPNI, including a requirement that all 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.

Alltel 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 Alltel their account number and mobile number. The post paid 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. Post paid 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, post paid customers were required to utilize their user identification and password for online access to CPNI.

My Account registration for Alltel business customers required two data elements in addition to the My Account registration process for post paid consumers. Business customers were required to provide their business' tax identification number to Alltel and to create a personal identification number (PIN) after they entered their user identification and password. For on-line access to CPNI after the registration for a business account was complete, users were required to submit their user identification, password and PIN.

Alltel prepaid customers registered for online access to CPNI in the same manner as described above. Prepaid 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, prepaid customers were required to utilize their user identification and password for online access to CPNI.

Additionally, Alltel 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 or Forgotten Passwords.**

Alltel made available a backup authentication method for customers who had forgotten their My Account password. This backup authentication method did not prompt the customer for readily available biographical or account information. If the 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 Alltel prior to establishing a new password.

### **(5) Notification of Account Changes**

Alltel 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. Alltel did not reveal the changed information.

### **(6) In-Store Access to CPNI**

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

### **H. Notification of CPNI Security Breaches**

Alltel's existing processes ensured compliance with the CPNI rules. Periodic meetings were conducted among Alltel's corporate security team and Trust Legal staff to consider internal investigations involving potential CPNI breaches. Alltel reported confirmed CPNI breaches and notified customers in accordance with the CPNI breach notification rules.

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

During the relevant period Alltel's physical security group completed 16 data breach series investigations; of these, 13 originated from complaints from customers regarding the unauthorized release of CPNI. Alltel's corporate security group investigated these complaints and 12 of them did not appear to result in improper access to or unauthorized release of CPNI. There were 4 instances of apparent improper access and improper disclosure by employees to unauthorized individuals.

### **J. Action Taken Against Data Brokers**

During the Relevant Period, Alltel did not initiate any actions against data brokers.