



**Qwest**  
607 14<sup>th</sup> Street, NW, Suite 950  
Washington, DC 20005  
Phone 303-383-6651  
Facsimile 303-896-1107

**Kathryn Marie Krause**  
Associate General Counsel

March 1, 2011

***FILED VIA ECFS***

Ms. Marlene H. Dortch  
Secretary  
Federal Communications Commission  
Room TW-A325  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

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

Dear Ms. Dortch:

Pursuant to the Federal Communications Commission's *Report and Order*,<sup>1</sup> Qwest hereby files its Annual 47 C.F.R. § 64.2009(e) CPNI Certification.

Please contact me at the above-listed information if you have any questions.

/s/ Kathryn Marie Krause

cc: Best Copy and Printing, Inc. ([fcc@bcpiweb.com](mailto:fcc@bcpiweb.com))

Attachment

---

<sup>1</sup> *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services, Report and Order and Further Notice of Proposed Rulemaking*, 22 FCC Rcd 6927 (2007). *Also see*, Public Notice, DA 11-159 (Jan. 28, 2011).

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

Annual 64.2009(e) Customer Proprietary Network Information (CPNI) Certification for 2011, covering the prior calendar year 2010.

Date filed: March 1, 2011

Name of companies covered by this certification:

Form 499 Filer ID:       808440 Qwest Corporation  
                              807684 El Paso County Telephone Company  
                              808882 Qwest Communications Company, LLC  
                              822734 Qwest LD Corp.

Name of signatory: Alwin Roberts

Title of signatory: Senior Vice President and General Manager–Mass Markets

I, Alwin Roberts, am an officer of Qwest Corporation (a local exchange carrier). Acting as an agent of that company, and on behalf of the other companies identified above (collectively Qwest), I certify that I have personal knowledge that these companies have established operating procedures that are adequate to ensure compliance with the Federal Communications Commission (FCC) CPNI rules. See 47 C.F.R. § 64.2001 *et seq.* My personal knowledge is based, in part, on the personal knowledge of those persons who represent to me that their organizations have procedures in place adequate to ensure compliance with the FCC's CPNI rules.

Attached to this certification is an accompanying statement (Exhibit 1) describing how the various companies have established operating procedures that are adequate to ensure compliance (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) with the requirements set forth in section 64.2001 *et seq.* of the FCC's rules.

**Actions Against Data Brokers.** None of the Qwest companies identified above took action in 2010 against data brokers either in courts or before regulatory bodies.

**Customer Complaints.** See Exhibit 2.

Acting on behalf of the above-identified companies, I represent and warrant that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The companies also acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject them to enforcement action.

Signed /s/ Alwin Roberts

[Electronic Signature]

Attachments: Accompanying Statement explaining CPNI procedures, Exhibit 1  
Summary of Customer Complaints, Exhibit 2

**EXHIBIT 1 TO COMPLIANCE CERTIFICATE**  
**Qwest Statement of Operating Procedures**

Below, Qwest describes its operating procedures to ensure compliance with the Federal Communications Commission (FCC) Customer Proprietary Network Information (CPNI) rules set forth in 47 C.F.R., Subpart U:

1. Alwin Roberts, Senior Vice President and General Manager in Mass Markets is Qwest's CPNI Certifying Officer. Once a year, Qwest utilizes a certification process in which the managers of those business units that might use CPNI for sales or marketing certify to Mr. Roberts that, based on their personal knowledge, their business and market units have practices and procedures in place to ensure compliance with the FCC's CPNI rules.
2. Qwest also takes advantage of the expertise and experience of a variety of its other (non-sales) organizational units and personnel in addressing privacy and CPNI issues. Qwest has a Chief Privacy Officer (CPO) within the Risk Management organization, whose duties include advice and counsel on a variety of privacy issues. Within that Risk Management organization there is also an Information Security and Technology group, and technical CPNI issues are vetted with it. Still within that organization, Qwest has a dedicated CPNI Compliance Manager with more than a decade of experience in addressing and counseling on the proper uses of CPNI. That Compliance Manager, along with other Qwest Risk Management employees, including the CPO and the Information Security and Technology group, is responsible for assisting Qwest business units on a host of issues, including product development, training, discipline and supervision of marketing campaigns. Finally, all of the Qwest employees referenced above interact with senior Qwest legal counsel on CPNI matters that require legal analysis or advice. That counsel has been involved in CPNI issues for over 25 years. Qwest is confident that this cooperative and collaborative cross-discipline approach to CPNI issues creates an atmosphere and structure that frame and support operating procedures adequate to ensure compliance with the FCC's CPNI rules.
3. To ensure that CPNI issues are resolved uniformly across the business and in a timely manner, the CPNI Compliance Manager hosts bi-weekly (and if necessary weekly) CPNI conference calls which are attended by senior CPNI legal counsel. When appropriate, members of the business units, Qwest's CPO, or other Qwest attorneys will attend these calls. During these calls, CPNI issues are discussed, issues are raised, solutions are reached and action plans are established. In addition, the CPNI Certifying Officer is consulted or advised as necessary.
4. In addition to the management structure addressed above that is designed to appropriately address CPNI issues, all Qwest employees receive training on CPNI rules. Employees with direct sales, marketing and product responsibilities receive more-detailed training on the proper use of CPNI than the employee base generally. This detailed training includes instructions on how to recognize and properly address CPNI issues during inbound sales calls, as well as instruction on outbound marketing campaigns, including how CPNI may and may not be used during such campaigns and what administrative records must be kept. Further, on an ongoing basis, targeted training is

conducted as needed. Additionally, in those cases where agents act as branded-Qwest representatives, Qwest provides appropriate training and scripting.

5. Beyond its formal training, Qwest has created CPNI "methods," available for all its employees that are likely to access, use or disclose CPNI. Those methods address, for example, how Qwest employees should deal with CPNI in the context of a telephone conversation or in a Qwest sales outlet. For example, the methods advise that employees should not disclose call detail records absent special customer verification (*i.e.*, a password), *unless* the customer provides the employee with specific details about the call in question so that the employee is responding to the information given by the customer. Those methods also state that in-store employees should not release CPNI to customers unless the customer presents a valid photo ID. Qwest publishes its methods internally for easy access and consultation and uses those methods in face-to-face training sessions, as well.
6. Qwest's practices and procedures advise that customers should not use biographical or account information to access CPNI online. Customers not exempt from the rules (*i.e.*, certain business customers) should authenticate themselves using a Qwest-issued security code to establish an online username and password. Additionally, Qwest has procedures regarding notifying customers when passwords, a response to a back-up means of authentication for a lost or forgotten password, online account, or address of record are created or changed. While Qwest's procedures are sound, available, and communicated to its employees (through training or internal posting), there are occasions where those procedures are not followed. In those cases, when Qwest is made aware of the matter, Qwest acts to resolve the departure from procedure and works with customers or employees to clarify Qwest's expectations.
7. Qwest sales personnel are required to obtain supervisory approval for their outbound marketing campaigns. They are required to maintain a record of their campaigns that use CPNI, including such details as: a description of the campaign (including the proposed dates and campaign purpose), the CPNI that was used and the products or services intended to be offered. The records are maintained for a minimum of one year.
8. Qwest, like other communications carriers, discloses CPNI to its agents for permissible marketing, fulfillment and provisioning activities. It also makes CPNI available to vendors who market Qwest's and their own services when those vendors have proof of authorization from the customer. These vendors generally sell "packages" of products, including telecommunications and information services, and customer premises equipment (CPE).
9. Qwest's primary systems used for sales and marketing allow a customer's CPNI approval status to be noted in customer records. Other than duration-of-the-transaction (call, email, visit, etc.) CPNI approval, Qwest uses opt-in approval mechanisms. A customer's CPNI approval can be changed by a customer at anytime by contacting Qwest.

10. Qwest engages in quality assurance programs that monitor calls for, among other things, compliance with the CPNI rules and correct customer authentication. That program provides feedback to managers for training purposes and, if appropriate, disciplinary action.
11. Qwest has documented disciplinary procedures regarding CPNI errors beyond its quality assurance program. A potential violation of CPNI rules is investigated, and, where appropriate, disciplinary action is taken.
12. Qwest requires its employees to report the unauthorized access, use or disclosure of CPNI to a central point, *i.e.*, its general internal advice line, for further investigation. Customer complaints sometimes also come to Qwest's attention through that line.
13. Qwest takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. Qwest performs routine security evaluations and security assessments on Qwest systems, including those containing CPNI. Additionally, the Information Security and Technology group performs external penetration tests on Internet-facing web portals to ensure proper security is maintained. These activities further ensure that the necessary information-security safeguards are maintained with respect to CPNI and other customer information.
14. Qwest works with law enforcement regarding unauthorized access, use or disclosures of CPNI or other customer information when appropriate, even beyond the requirements of the FCC's rules. With respect to the reporting of CPNI "breaches" under the FCC-mandated process (*e.g.*, to the Department of Justice portal), Qwest has a single point-of-contact employee who does that reporting. That employee first reviews the allegations and, after investigation, if a breach warrants reporting, she does the reporting. A log of such reports is maintained and Qwest will be maintaining these records for at least two years.
15. In 2010, Qwest updated its Privacy Policy and included a more lengthy discussion of CPNI than existed in its prior policies. The current Policy includes a link to the FCC's webpage that addresses CPNI and the Commission's rules.

**EXHIBIT 2 TO COMPLIANCE CERTIFICATE**  
**Qwest Statement of Customer Complaints**

Qwest investigated each of the 12 complaints summarized below. After an investigation, 1 was deemed unfounded, and 11 were deemed valid and reported to the Federal Bureau of Investigation (FBI) and United States Secret Service (USSS), through the portal established for improper CPNI disclosures.

Of the 12 customer complaints, 3 involved allegations of improper access to online information as a result of isolated incidents in Qwest's systems and 9 related to unauthorized access to a customer's account.

- ❖ 3 complaints were the result of isolated incidents in Qwest's systems, which have been resolved. Of these 3, 1 was unfounded.

June 14, 2010 - Between June 14 and 17, 2010, Qwest received complaints from three customers who were able to view another customer's account information in one of Qwest's self-service web portals for business customers. Qwest immediately investigated and fixed the problem, and has received no other complaints about it.

July 11, 2010 (Unfounded) - As a result of a system release for Qwest's MyAccount on July 11, 2010, it was reported that some customers may have been able to view other customer's data. Upon investigation, Qwest determined that individual customer information could not be viewed.

September 14, 2010 - Qwest provides a portal for business customers to manage their services. A user must log into it with a username and password. The portal includes the ability to manage 8xx numbers for those who buy Qwest 8xx services. A specific 8xx number was part of the URL address for portal access about that number. Due to a design flaw, once an authorized user with 8xx services entered the portal, that user could change the 8xx in the URL address of a page about one of its numbers to an 8xx number that was part of another account and see basic information about the services for that number. The available information did not include call detail records. The unauthorized user could make changes to certain description fields and other service settings. But those changes could not affect the operation of the service or the routing of calls. We know of one user who saw 8xx account information for a number on another account. Qwest has resolved this problem and it is no longer occurring.

- ❖ 9 complaints related to alleged unauthorized access to a customer's account.

January 4, 2010 - A customer contacted Qwest via email related to a billing matter on the customer's account. The email included information about the services the customer subscribes to, but no call details. The Qwest employee who received the email misunderstood it and thought it was related to pay phone service provided by another company. As a result, the Qwest employee forwarded the email to a contact he had at the pay phone company. We have provided the employee involved additional training on the appropriate handling of customer information and resolved the issue to the satisfaction of the

customer, who had previously become aware of the improper forwarding of the account information and contacted us about it.

March 9, 2010 - Over the course of two calls, Qwest customer service representatives provided an unauthorized party pretending to be a Qwest employee a non-published customer's name and address, and confirmed the name of the customer's long distance calling plan. The unauthorized caller already had the customer's non-published telephone number prior to contacting Qwest. The account information that was provided did not include any call details. The customer was notified and we provided additional training to the customer service representatives involved to follow our clearly established authentication procedures.

March 10, 2010 - As a result of a customer complaint, Qwest filed a general report regarding unauthorized release of CPNI in those situations where an incorrect telephone number is entered into an interexchange or local carrier's systems in connection with a customer's change of interexchange carrier. This can happen a number of ways. For example, a customer could give the wrong number when asking for a carrier change or the person taking the order could mis-enter it. In such cases, the carrier's systems would have the right customer name and address on the account but the wrong telephone number. As a result, call detail associated with the wrong number listed on the account would be billed to the customer identified in the carrier's systems. Generally, the customer receiving the billing information will recognize that it is wrong, or the customer making the calls in question will notice the lack of charges, and contact their carrier to get the matter resolved.

March 29, 2010 - Qwest sent out scheduled maintenance email notifications to customers reflecting their Qwest circuit ID numbers and service types. Due to a change in the notification system, 41 customers received circuit ID and service type information for services other than their own. This error was corrected.

May 20, 2010 - A customer apparently provided our sales consultant an incorrect email address during the order process. As a result, we sent an order confirmation, including a summary of the services ordered to the incorrect email address. In this instance, the incorrect email address happened to belong to a Qwest employee. The email address was corrected.

July 12, 2010 - During the initial set up of an account, our customer service personnel entered an inaccurate customer email address in our records. As a result, we sent an order confirmation and other order related information to the incorrect email address. Those materials may have included CPNI. The recipient of the emails notified us of the problem. The account for which the confirmations were sent has since been disconnected.

August 30, 2010 - One of our sales consultants made a mistake while assisting a customer with a question about online account access. The consultant wrongly provided the customer access information for another account that previously had the same telephone number, and also linked the accounts together in our systems. As a result, the customer advised Qwest that she was able to see information on the other account. We fixed the problem. The customer can no longer see the other account information. And we re-enforced training in our

sales and care organizations about how to address problems with online account access when a customer has a telephone number that was previously assigned to another account.

September 15, 2010 - A customer contacted Qwest regarding a billing error on her account. We added wireless service billing to her account in error. As a result, that customer saw the wireless plan and information about total minutes of use associated with a different customer (but no call detail). These types of errors occur from time to time and are the result of human error (for example, wrong telephone number or account information inputted into Qwest systems), which results in charges (sometimes reflecting CPNI) being associated with and disclosed to a wrong customer. These errors are similar to those that might occur when a customer is establishing or changing long distance providers. The errors are infrequent and we correct them when we become aware of them, as we did in the case referenced here.

September 21, 2010 - A customer contacted Qwest advising that she could see another customer's account. In error, an employee added one customer's account to the online profile for another customer's account that previously had the same telephone number. As a result, each customer could view information about the other's account. We have disassociated the accounts and resolved the problem. We are reinforcing training for employees working with online account profiles, especially in circumstances involving reassigned telephone numbers.