Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the	)	CC Docket No. 96-115
Telecommunications Act of 1996:	)	
	)	
Telecommunications Carriers' Use	)	
of Customer Proprietary Network	)	
Information and Other Customer Information	)	

**COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.
TO ADDITIONAL CUSTOMER PROPRIETARY
NETWORK INFORMATION RULEMAKING**

Craig J. Brown
Kathryn Marie Krause
Suite 950
607 14th Street, N.W.
Washington, DC 20005
303-383-6651

Attorneys for

QWEST COMMUNICATIONS
INTERNATIONAL INC.

April 28, 2006

TABLE OF CONTENTS

Page

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Implementation of the	)	CC Docket No. 96-115
Telecommunications Act of 1996:	)	
	)	
Telecommunications Carriers' Use	)	
of Customer Proprietary Network	)	
Information and Other Customer Information	)	

**COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC.
TO ADDITIONAL CUSTOMER PROPRIETARY
NETWORK INFORMATION RULEMAKING**

Like the Federal Communications Commission ("Commission" or "FCC"), Qwest Communications International Inc.[1] ("Qwest") "has long been committed to safeguarding customer privacy."[2] While Congressional oversight of Customer Proprietary Network Information ("CPNI") did not occur until 1996, Qwest -- a successor to U S WEST and now a Bell Operating Company ("BOC") -- has long had its use of CPNI regulated by the Commission.[3] But even before federal regulation of CPNI, Qwest had a history of protecting its

[1] This filing is made on behalf of Qwest Communications International Inc.'s common carrier companies, specifically Qwest Corporation (local exchange), Qwest Communications Corporation (long distance) and Qwest Wireless, Inc., collectively referred to as Qwest. In the event a point is being made with respect to a single company, that company will be identified by name.

[2] These Comments are filed in response to the Commission's most recent rulemaking *Notice*, released on February 14, 2006. *In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Petition for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information*, CC Docket No. 96-115 and RM-11277, Notice of Proposed Rulemaking, 21 FCC Rcd 1782, 1782-83 ¶ 1 (2006) ("*Notice*").

[3] As acknowledged in the *Notice*, prior to the 1996 Act, the Commission regulated the CPNI of BOCs under its *Computer II*/Open Network Architecture ("ONA") regulatory regime. *Id.* at 1782-83 n.2, wherein the Commission references the *1998 CPNI Order*, which describes the Commission's privacy protections (and includes the relevant citations) for confidential customer

customer information. After all, customer information allows for educated and responsive communication between a carrier and its customers, as well as accurate billing and revenue generation. As such, customer information is a substantial common carrier asset. Protecting that asset is integral to the trust between a carrier and its customers, as well as a critical component of management's fiduciary obligation to its shareholders.

Prior to the AT&T divestiture over two decades ago, and continuing to this day, Qwest has acted to protect its customer information and to release that information only when it appears reasonable and appropriate to do so. To that end, Qwest has put into practice methods and procedures, as well as security tools and controls to support and confirm Qwest's dedication to protecting information about its customers and their associated privacy interests.

It is from this tradition and within its current business climate that Qwest comments here and opposes the government mandates proposed by the Electronic Privacy Information Center ("EPIC") in its Petition for Rulemaking ("EPIC Petition" or "Petition").[4] Qwest urges the Commission to conclude this rulemaking with a finding that carriers already are subject to the right balance of CPNI regulatory oversight; and that most carriers have responsible safeguards in place with regard to access, use and disclosure of CPNI. Alternatively, the Commission might

---

information in place prior to the 1996 Act. *See In the Matter of Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of the Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as amended*, CC Docket Nos. 96-115 and 96-149, Second Report and Order and Further Notice of Proposed Rulemaking, 13 FCC Rcd 8061, 8068-70 ¶ 7 and associated footnote references (1998) ("*1998 CPNI Order*"), *on recon.*, 14 FCC Rcd 14409 (1999) ("*CPNI Reconsideration Order*"), *vacated sub nom. U S WEST v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213 (2000) ("*U S WEST v. FCC*").

[4] Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115, filed Aug. 30, 2005 ("EPIC Petition").

pronounce guidelines that would frame a safe harbor for carriers incorporating those guidelines into their operating practices.

I. INTRODUCTION AND SUMMARY: EPIC'S PROPOSALS MIGHT BE APPROPRIATE AS ADJUDICATIVE REMEDIES, BUT NOT AS RULES

The Commission's *Notice*, like EPIC's Petition, addresses matters of serious and legitimate public concern: the fraudulent procurement of customer information from carriers by persons pretending to be customers or someone authorized by the customer. The conduct is not only disturbing,[5] it is outrageous and often illegal. Data brokers who engage in pretexting should face the full wrath of regulatory agencies.[6] But regulatory reaction should be confined to those bad actors, or to carriers demonstrably lax about their information security, customer authentication or information-disclosure practices. Costly and operationally burdensome government regulations should not be inflicted on well-intentioned carriers in the absence of proven public interest benefits. EPIC has failed to prove that carriers, acting in conformity with established and sensible business practices to secure CPNI and to screen customers before discussing account information, should be saddled with such costs and administrative interference.[7]

Qwest, like all businesses accumulating customer account information and having routine customer contacts, strives to provide responsive, quality service in an "easy-to-do business with"

---

[5] After describing the activities of data brokers, the *Notice* "find[s] this conduct to be very disturbing." *Notice*, 21 FCC Rcd at 1782-83 ¶ 1.

[6] *See* Comments of Kim Phan, CC Docket No. 96-115, filed Apr. 14, 2006 at 7 ("Kim Phan EPIC Petition Comments") ("As there are no known legitimate methods of obtaining this information that does not involve fraud, misrepresentations or some other violation, the perpetrators of these illegitimate methods are the ones responsible for creating this threat to consumer privacy, and measures should be taken to pursue these individuals.").

[7] *See id.* at 1 ("EPIC has overstated the value to consumers of imposing enhanced security and authentication standards on . . . carriers.").

environment. And Qwest, like all other businesses that manage account information, strives to balance customer convenience with necessary customer authentication and other security protections. Achieving the right balance is as much art as science.[8] To determine the right balance, carriers like Qwest must consider a multitude of factors, including: (1) the volume of customer transactions they experience per week or per month or per year; (2) customer partiality for ease and convenience; (3) the nature of the risks involved, *e.g.*, "Are the risks occurring now or anticipated?"; "If now, what is the likelihood, frequency or the regularity of the risks?"; "What is the ability to manage the risks after they occur rather than in anticipation of them?"; and (4) the overall costs to the business and its customers of acting now, acting later or not acting at all. There is no perfect balance, no "one-size-fits-all" model. Rather, there are judgments and exercises of discretion that carriers should be accorded the right to make.

In the absence of a proven pattern of carrier conduct evidencing inadequate business practices or security protections, or facts evidencing carrier complicity with fraudulent conduct, carriers -- like other commercial businesses -- should be free to balance the costs and benefits of particular security measures when designing and implementing their information security architectures and protecting their informational assets, including customer information. Barring proof of significant carrier negligence or carelessness, the federal government should not impose business rules on the carrier-customer relationship that are not driven by product and service considerations and are not borne by other service providers or industries.

---

[8] *Compare id.* at 3 ("Telecommunications carriers must walk a thin line between meeting their obligation to offer customer access to CPNI while protecting CPNI from all the rest of the world."), *id.* at 8 ("Any increase in the security measures put into place should not be so overly complicated or cumbersome that it prevents or inconveniences customers from obtaining their own confidential account information.").

EPIC provides no proof of carrier negligence or carelessness. Rather, it makes an argument in the nature of the tortious concept of *res ipsa loquitur*, *i.e.*, "the thing speaks for itself."[9] The "thing" EPIC alleges is not disputed, *i.e.*, that data brokers have possession of some carrier customer records.[10] It is the "speaks for itself" aspect of the equation that Qwest disputes -- that *unless* a carrier failed to be diligent with regard to its customer records or had acted irresponsibly with respect to the release of such records, data brokers would not have possession of CPNI.[11]

The tortious framework EPIC employs is ill suited to the facts EPIC professes concern about. It is not necessarily true (that is, it does *not* "speak for itself") that a carrier lacks diligence or has behaved without due care if some of its customer information ends up in the hands of a fraudster. It is not necessarily the case that a carrier is at fault if it is duped out of information by a fraudulent impersonator maliciously preying on the good intentions of the carrier's employees and their desire to be helpful to a customer. Given EPIC's failure to prove that the problems it describes reflect broad-based carrier malfeasance, it would be exceedingly

---

[9] This approach is adopted as well by the Privacy Rights Clearinghouse, *et al.*, whose comments in this proceeding begin with the undemonstrated remark that the data broker matter "point[s] to a disturbing situation: Not only are current safeguards for customer calling records inadequate, but those that exist are being blatantly ignored." Comments of Privacy Rights Clearinghouse, *et al.*, dated Apr. 24, 2006 at 2. The Comments continue: "The fact that there are many web sites offering phone records for sale is an indication that current safeguards are inadequate and that carriers need to do more." *Id*. at 3.

[10] The Commission notes, and Qwest concedes, that EPIC provided facts regarding data brokers holding themselves out as being in possession of certain information and offering it for sale. *See Notice*, 21 FCC Rcd at 1786-87 ¶ 10 ("EPIC has supplied information to the Commission to support its contention that numerous data brokers and private investigators widely advertise their ability to obtain CPNI without the account holder's knowledge and consent.").

[11] *See* CTIA – The Wireless Association Comments in Opposition to EPIC Petition for Rulemaking, CC Docket No. 96-115, RM-11277, filed Oct. 31, 2005 at 2 ("CTIA EPIC Petition Comments") ("The EPIC Petition assumes incorrectly that such records may only be obtained through lax carrier security procedures.").

bad public policy for regulators to overlay a gloss of presumed carrier negligence on situations where fraud is being perpetrated on carriers themselves.

The impropriety of *presuming* carrier misconduct in the current context is made more pronounced by the lack of alignment between EPIC's proffered remedies and its articulated complaints. With the exception of EPIC's "customer-chosen password" proposal, there is scant correlation between its proposals and the protection of customer information from data brokers intent on acquiring such information fraudulently. It is impossible, for example, for advocates such as EPIC to craft a meritorious case for in-storage encryption of data held by carriers when such encryption is not an integral aspect of information security controls even in the financial sector. And EPIC provides no logical explanation for why communications carriers should be encumbered by regulations mandating elaborate audit-trail functionalities when most commercial enterprises that collect, use, disclose and store data often as sensitive as CPNI are not similarly encumbered.

The Commission should not prescribe additional CPNI rules along the lines proposed by EPIC. Rather it should take one of two actions short of that. Qwest's preference would be for the Commission to end this proceeding with a finding that the current CPNI rules with their associated safeguards already provide the appropriate regulatory "framework [that] calibrates the protection of . . . information from disclosure and dissemination based on the sensitivity of the information."[12] Such action would avoid imposing significant costs on carriers and their customers with respect to a problem that seems already to be waning in some degree due to actions by the Commission, the Federal Trade Commission ("FTC"), private litigants, adverse publicity and threatened legislation. The number and range of remedial actions is a testament to

[12] *Notice*, 21 FCC Rcd at 1783 ¶ 2.

the fact that bad actions can be curbed short of industry-wide government mandates confined to telecommunications common carriers.[13]

Alternatively, the Commission might promulgate guidelines that would form a safe harbor, along the lines incorporated in the Commission's Telephone Consumer Protection Act ("TCPA") rules.[14] Such guidelines might require carriers to file their CPNI Certifying Officer's Certificates with the Commission, rather than simply making them available for public inspection. There might be a requirement that carriers establish and maintain written policies for customer authentication. The guidelines might require carriers to extend to customers that want passwords the ability to use them. Carriers that incorporated the Commission's guidelines into their operating practices would not be liable for occasional CPNI-rule violations. Enforcement action would be reserved for and targeted to specific carriers who repeatedly failed to properly safeguard CPNI.

Within an enforcement model, the Commission might incorporate some of the ideas reflected in the EPIC Petition as elements in a consent decree or findings of liability. But absent compelling evidence of widespread unjustifiable conduct by a larger number of carriers, the industry should be free of additional government regulations with potentially crushing costs,

---

[13] Among the actions that appear to be stemming data broker activity is EPIC's own filing with the FTC (*In the Matter of Intelligent e-Commerce, Inc.*, Complaint and Request for Injunction, Investigation and Other Relief, dated July 7, 2005, filed as an attachment to the EPIC Petition). There have also been lawsuits filed by T-Mobile, Verizon, Sprint/Nextel, Cingular. *See* Kim Phan EPIC Petition Comments at 18 (referencing the various litigation activities). *And see Remsburg v. Docusearch, Inc.*, 816 A.2d 1001 (N.H. 2003) (holding that a data broker is potentially liable for harms caused by selling personal information, not the source that disclosed the information). And there has been a variety of legislative proposals regarding the matter. *See* Kim Phan EPIC Petition Comments at 16-17 (noting that at least eight bills have been introduced in Congress within the past few months).

[14] 47 C.F.R. § 64.1200(c)(2).

costs that would be passed from the carrier onto their customers in the form of higher prices or reduced services. The public deserves better.

II. EPIC'S PROPOSALS DO NOT ALIGN WELL WITH THE GOAL OF ELIMINATING FRAUD BY DATA BROKERS

In Section III below, Qwest outlines some of its broad range of internal controls regarding access, use and disclosure of CPNI. The controls include technological and electronic ones, employee training and discipline, and accommodating customers' requests for passwords when they feel the need for them.

But suffice it to say here that EPIC provided no credible proof rebutting the adequacy of existing carrier information security controls. Just the contrary. EPIC acknowledged that it could point to no instance of carrier misconduct.[15] This is not surprising. After the passage of the Sarbanes-Oxley Act of 2002 ("SOX"),[16] those claiming that a publicly-held company's security controls pertaining to financial systems and data (which included significant amounts of customer information) are inadequate would have an exceedingly difficult time proving it. Such companies are required to have adequate controls in place to ensure the confidentiality and integrity of financial information, supported by an annual certification from an internal controller and an attestation from an independent body.[17] In a very material way, SOX buttresses those CPNI safeguards that the Commission itself established.

---

[15] *Notice*, 21 FCC Rcd at 1786-87 ¶ 10 ("EPIC does not claim it knows specifically how these online data brokers . . . are obtaining unauthorized access to CPNI.").

[16] 15 U.S.C. § 7262.

[17] *See also* CTIA EPIC Petition Comments at 7-8 (discussing the SOX controls and their relevancy to carrier practices).

But the benefit to EPIC of its chosen advocacy approach is that it permits EPIC to simply point to an unfortunate set of facts, draw broad unproven conclusions,[18] and propose costly government intervention. For Qwest to implement EPIC's proposals in their entirety would afflict it with many millions of dollars in costs to design, implement and maintain the necessary systems, repositories, software and hardware.[19] Compliance efforts would divert scarce, valuable human and monetary resources[20] from what should be carriers' primary business drivers and focus -- innovation, state-of-the-art products and services, and customer care.

Below, Qwest addresses more specifically EPIC's proposal as described in the *Notice.* EPIC's proposals are not measured, are not aligned with the problem EPIC complains about, and will not remedy the problem of fraudulent data broker conduct.[21] Moreover, even where there is some logical connection between an EPIC proposal and the data broker problem, EPIC fails to show why the Commission should compel all telecommunications carriers to adopt particular business practices in the absence of any showing even now that a single carrier's practices are beyond the realm of reasonableness. Without such a showing, the "comprehensive set of rules"

---

[18] *Compare Notice*, 21 FCC Rcd at 1786 ¶ 9 ("As noted . . . EPIC *alleges* that the Commission's CPNI regulations are insufficient to prevent the unauthorized disclosure of CPNI"), at 1786-87 ¶ 10 ("EPIC *suggests* [one set of possibilities for how data brokers secure access to carriers' customer records is] possibly through dishonest insiders at the carriers. EPIC *suggests* that unauthorized third parties are exploiting existing security standards") (emphasis added).

[19] *Compare* Comments of Verizon, RM-11277, filed Oct. 31, 2005 at 4-5 ("Verizon EPIC Petition Comments) (Verizon predicted that the costs just for EPIC's document retention and encryption proposals would "likely . . . cost the industry hundreds of millions of dollars to develop and implement.").

[20] *See* Kim Phan EPIC Petition Comments at 13 ("Carriers should be allowed to focus their scarce resources on actually preventing those wrongdoers from perpetrating the harm rather than being forced to expend increasing amounts of money to comply with perfunctory administrative costs.").

[21] *See* Comments of the Public Service Commission of the State of Missouri, CC Docket No. 96-115, RM-11277, undated, at 2 ("MoPSC EPIC Petition Comments") ("the MoPSC questions whether [EPIC's proposals] will provide the desired level of security given the current actions and claims of entities currently obtaining unauthorized access to CPNI.").

the Commission has already adopted regarding CPNI are quite sufficient.[22] And were an advocate like EPIC to demonstrate that a specific carrier was acting unreasonably or irresponsibly, targeted enforcement would be the more rational regulatory tool.

A. In-Storage Encryption Cannot Be Supported By Any Rational Cost-Benefit Analysis

Of all the EPIC proposals discussed in the *Notice*, EPIC's proposal for encryption of data in-storage data is the most attenuated from the problem of fraudsters seeking information from a carrier either over the telephone, on-site or on-line. Encryption in storage is not a standard information control practiced by businesses generally. Such encryption protects only against certain kinds of data theft and hacking incidents, not the kind of conduct most likely forming the basis for unauthorized third parties seeking to obtain CPNI from carriers.[23]

Encryption of data in storage has limited usefulness in preventing pretexting because the in-storage encrypted information has to be unencrypted for an employee to use it, discuss it with, or disclose it to, a customer *or* for a customer to easily retrieve the information his/herself (such

---

[22] *Notice*, 21 FCC Rcd at 1784 ¶ 5. *And see id.* at 1785 ¶ 7 and n.16 (noting that the Commission has already "adopted a set of rules designed to ensure that telecommunications carriers establish effective safeguards to protect against unauthorized use or disclosure of CPNI," citing to *1998 CPNI Order*, 13 FCC Rcd at 8195 ¶ 193).

[23] *See* MoPSC EPIC Petition Comments at 3 (noting that "[t]he same failings [of EPIC's proposals] applicable to [ ] customer-set password[s] . . . would apply to encryption.").

Qwest is aware of occasional references to hacking or hackers in some of the data broker litigation, although it is doubtful that substantial evidence will be proffered that the current problem with data brokers possessing CPNI happened because of hacking. References to hacking or hackers can be found in connection with the Cingular cases against Data Find Solutions and First Source, Civil Action File No. 1:05-CV-3269-CC, in the United States District Court for the Northern District of Georgia, Atlanta Division. *See* Cingular's "Complaint for Preliminary and Permanent Injunctive Relief, Replevin, and Disgorgement" (at p.9 ¶ 24, p.18 ¶ 64, p.19 ¶ 68), "Brief in Support of Cingular Wireless LLC's Motion for Temporary Restraining Order" (at p.5) and "Declaration of Kathleen Rehmer" (at p.5 ¶¶ 17-18).

as on-line).[24] It is at the point of disclosure or retrieval -- not while the data is in storage -- that most of the risks associated with pretexting evidence themselves.

A telecommunications regulator should decline to mandate encryption of data in storage when not even regulators of financial institutions have required such encryption.[25] Given that there is no such compulsion in the financial sector, where the customer account information is at least as sensitive as CPNI,[26] those (like EPIC) urging the adoption of such encryption in the communications industry should have to make a compelling case to support their position.

---

[24] *See* Comments of the Public Utilities Commission of Ohio, CC Docket No. 96-115, RM-11277, filed Apr. 13, 2006 at 14 ("Ohio PUC EPIC Petition Comments") (after noting that encryption might provide some degree of protection, stating that "However, encryption may be of limited practical use, since the information must be decrypted at some point within the carrier's computer systems").

[25] *See Guin v. Brazos Higher Education Service Corporation, Inc.*, 2006 U.S. Dist. LEXIS 4846 (D. Minn. 2006) (holding that the Gramm-Leach-Bliley Act ("GLB") did not require encryption of information on a lap-top computer; and noting that while the FTC appears to routinely caution "businesses to 'provide for secure data transmission' when collecting customer information by encrypting such information 'in transit,' there is nothing in the GLB Act about this standard, and the FTC does not provide regulations regarding whether data should be encrypted when stored on the hard drive of a computer.").

[26] "Prepared Statement of the Federal Trade Commission, Before the Committee on Commerce, Science, and Transportation Subcommittee on Consumer Affairs, Product Safety, and Insurance, U.S. Senate, on Protecting Consumers' Phone Records," authored by Lydia B. Parnes, Director of the Bureau of Consumer Protection of the FTC, dated February 8, 2006 at 7 ("Although the acquisition of telephone records does not present the opportunity for immediate financial harm as the acquisition of financial records does, it nonetheless is a serious intrusion into consumers' privacy and could result in stalking, harassment, and embarrassment.") (footnote omitted). Ms. Parnes stated that the "views expressed in [her] statement represent[ed] the views of the Commission."

The fact that CPNI is sensitive information[27] does not end the inquiry. Unless CPNI is being stolen by hackers from telecommunications carriers on a widespread basis, encryption in storage is an overreaction to the problem. Only if the costs and benefits of such information security control were fairly balanced could there be a regulatory "framework [that] calibrates the protection of . . . information from disclosure and dissemination based on the sensitivity of the information" itself.[28] Encryption of data in storage is a proposal out of balance with the data broker problem and the public interest, since the costs of developing and implementing this tool would far outweigh any probable public benefit.

The fact that most carriers probably do not have encryption of data in storage capabilities at this time does not threaten the reasonable security of CPNI. Qwest considers its existing information security controls to be robust, responsible, and effective. These controls protect Qwest's confidential information, including its customer information, against hacker-created breaches and theft. While Qwest does not routinely encrypt data in storage, it does use encryption as an information security control and tool in those cases where it makes sense as an industry-standard, responsible practice, *e.g.*, encrypting data in-transit, especially data associated with Internet communications.

In Qwest's opinion, an investment to design and implement encryption-in-storage functionalities would be an imprudent investment at this time, from the perspective of balancing competing business and customer needs. Because there is no proof that the public would be

[27] *See, e.g., 1998 CPNI Order*, 13 FCC Rcd at 8135-36 ¶ 97; Written Statement of Kevin J. Martin, Chairman, Federal Communications Commission; Hearing on Phone Records for Sale: Why Aren't Phone Records Safe from Pretexting? -- in connection with Testimony before the Committee on Energy and Commerce, U.S. House of Representatives, 2006 FCC Lexis 462 (Feb. 1, 2006) ("[W]e are initiating a proceeding to determine what additional rules the Commission should adopt to further protect consumers' sensitive telephone record data. . ."). *And see U S WEST v. FCC*, 182 F.3d at 1235-36.

[28] *Notice*, 21 FCC Rcd at 1782 ¶ 2 (discussing the range of sensitivity of CPNI).

served by the Commission's forcing carriers to make such an investment, the Commission should reject the proposal.

B. Mandated Audit-Trail Controls Should Be Reserved For Enforcement Actions

As with EPIC's encryption of data in storage proposal, EPIC similarly fails to demonstrate how its recommended audit-trail proposal is aligned with meaningful consumer benefit. This is a material failing in light of the fact that many carriers already have some form of audit-trail capabilities.[29] Larger carriers' audit functionalities, functionalities shared by Qwest, can generally track when an employee accesses a system or database and when he/she leaves. This information can later be used to discern whether a particular employee accessed a particular system with -- or without -- authorization.[30] Such information can be used, in turn, to ensure that employees who are *not* authorized to access systems that contain customer information do not do so. And if some employees do act contrary to established carrier practices, they will be subject to the carrier's express disciplinary plan,[31] which likely would include dismissal where warranted.

Beyond audit functionalities that record basic employee entry into and exit from a system, many carriers likely have more sophisticated audit controls. Larger carriers, like Qwest,

---

[29] The BOCs, and later GTE, were required by the Commission's *Computer II* and ONA rules, to incorporate password-identification protection in to their "primary" customer information databases. *See, e.g., In the Matter of Filing and Review of Open Network Architecture Plans*, Memorandum Opinion and Order, 8 FCC Rcd 2606, 2610 ¶ 18 (1993); *In the Matter of Filing and Review of Open Network Architecture Plans*, Memorandum Opinion and Order, 5 FCC Rcd 3103, 3118-19 ¶¶ 129-37 (1990).

[30] MoPSC EPIC Petition Comments at 3 ("Audit trails are useful when tracking and prosecuting entities that obtain consumer telephone records dishonestly or inappropriately. However, audit trails do little *to prevent* the unauthorized release of consumer information." (emphasis added)).

[31] 47 C.F.R. § 64.2009(b); *1998 CPNI Order*, 13 FCC Rcd at 8198 ¶ 198; and *Notice*, 21 FCC Rcd at 1785 ¶ 7 and n.18.

might have audit tools that "mark" a specific record with a unique employee identifier when an employee accesses a customer account. And like Qwest they might have audit technology that tracks not only the fact that a service representative accessed an account (*e.g.*, a log of entry/exit) but also requires notes explaining the reason for access to the customer record, as well as any action taken.[32]

Based on the record compiled in response to the *Notice*, the Commission might determine it appropriate, as part of a safe harbor structure, to include a requirement that carriers attest to and describe some basic audit functionality in connection with CPNI access, use and disclosure. But the Commission should act cautiously with respect to mandating particular kinds or types of audit capabilities. It is highly unlikely that carriers, even larger carriers, have current audit capabilities that allow them "to record all instances when a customers' records have been accessed, whether information was disclosed, and to whom."[33] And this is not at all surprising

[32] *Compare* Comments of Verizon Wireless, RM-11277, filed Oct. 31, 2005 at 7 ("Verizon Wireless requires customer service representatives to record all instances when a customer's record is accessed, the subject of the discussion with the customer, and whether they have disclosed any information to the customer. This type of recording is important for purposes of customer service, and it is also helpful in investigating security breaches."). *And see* Testimony of the Honorable Steve Largent, President and Chief Executive Officer, CTIA – The Wireless Association, Before the U.S. Senate Subcommittee on Consumer Affairs, Product Safety, and Insurance, "Protecting Consumers' Phone Records," February 8, 2006 at 7 (service representatives "are trained to annotate the customer record whenever an account change or event occurs. A [representative] will note when a customer called and asked for his or her records.").

In those instances where a Qwest employee fails to leave a note, Qwest's system logs a note that entry was done but does not provide a reason.

[33] *Notice*, 21 FCC Rcd at 1789-90 ¶ 17. Qwest believes that if there are carriers that have deployed the kinds of audit capabilities that EPIC proposes, they are likely to be newer, smaller carriers not burdened by legacy systems from a number of different operating carriers, utilizing a wide variety of technologies, across a span of geographies.

since the Commission rejected the imposition of these kinds of extensive[34] audit trails in 1999.[35] And while it may be true that data storage costs are not as high now as they were in 1999, Qwest believes it would still be true that the kind of audit-trail functionality proposed by EPIC would require -- across the telecommunications industry -- "'massive' data storage requirements at great cost,"[36] along with costs for extensive updates to existing application software.

Carriers would incur initial costs to build repositories to house audit-trail detail and associated analytics. The burden would continue through recurring annual costs for maintaining and upgrading those repositories.

There would also be significant costs associated with collecting the information that was to be stored for later auditing. The information would have to be collected electronically, technologically tracking every click and stroke of those interacting with CPNI; or service representatives would have to capture the most relevant information regarding CPNI access and disclosure in a written narrative or by populating fields on a screen. The electronic model (the collect everything model, along the lines proposed by EPIC) simply bears no reasonable relation to most carriers' business needs, and its expense would cripple the telecommunications industry. The human labor/electronic input model creates audit information in real time, materially increasing the customer's holding times (*i.e.*, the service representative would be talking and recording in the same transaction) or time to answer (*i.e.*, because each call takes longer, less

[34] *CPNI Reconsideration Order*, 14 FCC Rcd at 14474-75 ¶ 127 (the audit "requirement was broadly intended to track access to a customer's CPNI account, recording whenever customer records are opened, by whom, and for what purpose.").

[35] The Commission eliminated its audit trails mandate in order "to reduce burdens on the industry while [still] serving the purposes of the CPNI rules." *Id.* at 14469 ¶ 18.

[36] *Id.* at 14474-75 ¶ 127 (quoting letter from Judy Sello, Senior Attorney, AT&T to Carol Mattey, Chief, Policy & Program Planning Division, Common Carrier Bureau, dated Jan. 12, 1999. The *CPNI Reconsideration Order* referenced carrier-cited costs of at least $364.6M (plus 'many millions' more) to comply with the audit requirement. *Id.* at 14471-72 ¶ 124.

calls get answered). In some cases, carriers could be subject to state regulatory penalties for delays associated with these kinds of information-tracking activities.

Finally, there is the practical -- and not theoretical -- scope issue of what information a carrier would have to track or log, and in what contexts. For example, would a field technician talking to a person at a service address associated with the account holder be required later to fill out some form to be input into some database if he/she disclosed CPNI in answer to a customer's question? What if there were an unidentified third party in the room? The problem is obvious.

In closing, it is as true today as it was in 1999 that "it is already incumbent upon all carriers to ensure that CPNI is not misused and that [the Commission's rules] regarding the use of CPNI are not violated . . . [O]n balance, such a potentially costly and burdensome rule [as that urged by EPIC] does not justify its benefit."[37]

C. Carriers Retain Data So Long As The Business Needs The Records

EPIC proposes that the Commission establish rules requiring carriers to delete customer record information when the information is no longer needed for billing or dispute resolution purposes.[38] Alternatively, EPIC proposes that carriers "de-identify" records by separating the identity of a person from the general transaction records. As framed, the Commission should reject both proposals.

There are a number of reasons why the Commission should decline to adopt a rule along the lines proposed by EPIC. Qwest highlights only three of them here. First, such a rule fails to resolve the problem the Commission is trying to address -- data brokers fraudulently securing

[37] *CPNI Reconsideration Order*, 14 FCC Rcd at 14474-75 ¶ 127.

[38] *Notice*, 21 FCC Rcd at 1790-91 ¶ 20.

current customer records from carriers.[39] Second, EPIC's proposed retention period is tied to a carrier's use of customer records only for two limited purposes: billing or dispute resolution. These uses are too narrow to reflect actual carrier needs for the records, as discussed below. Finally, EPIC's "anonymizing the records" alternative proposal would cost many millions of dollars for the telecommunications industry to implement with no associated public interest benefit.

Qwest, like other carriers, has implemented a formal records management policy, document retention schedule, and associated procedures that apply to all of Qwest's business operations, as required by 47 C.F.R. § 42. Customer information, such as call detail records, is considered sales and services records that Qwest keeps for a minimum of two years.[40]

Qwest often extends its default retention period as a result of legal or tax holds that override its general retention schedule. Because customer-usage detail information is of substantial significance to billed revenues, Qwest retains these usage detail/billing records for the amount of time associated with Internal Revenue Service or applicable state tax holds **plus** an additional year. This often leads to retention periods that can range from seven to fifteen years.

The Commission should reject EPIC's proposal. Qwest would not object to a customer-records retention requirement that was somewhat revised to accommodate legitimate, lawful carrier practices. Such a rule might require carriers to destroy or remove the records when there is no longer any business purpose served by their retention. But the Commission should not

---

[39] *See* MoPSC EPIC Petition Comments at 4 ("Limited date retention periods will reduce the amount of CPNI data at risk at any given time but does little to protect the information currently on file with a telecommunications carrier. Further, older CPNI that would be purged under [the EPIC] proposal, may be of little commercial use to those who obtain it improperly or illegally. It is a consumer's current information that is sought by entities improperly using the data. Therefore, such a requirement may be of little practical value.").

[40] *Compare* 47 C.F.R. § 42.6 (requiring carriers to maintain toll billing records for 18 months).

establish either a "use requirement" or a "maximum number of years" requirement for carrier records to be maintained where the records might be associated with a *bona fide* business purpose.

D. Notification To Customers Of Security Breaches

The *Notice* references EPIC's proposal to provide telecommunications subscribers with security breach notifications in the event CPNI is improperly disclosed.[41] The *Notice* states that Verizon Wireless previously opposed the idea, arguing that a notice requirement was unnecessary in part because "customers are already routinely notified of any known security breach."[42] While the *Notice* does not specifically seek additional comment on the propriety of subscriber notification *after* a security breach has occurred, it is not clear that the concept has been rejected either. For this reason, Qwest briefly addresses the notion below, then moves on to address other notification ideas raised in the *Notice.*

When Qwest suspects that a customer's account has been accessed without authorization, it investigates the matter. If the matter being investigated falls within the legislative mandates of a variety of state breach-notification laws, Qwest would do a notification. If there is no legislative directive requiring a notification, Qwest would make a case-by-case decision how to proceed with outreach to its customer or others. If a notification is done in these situations, it is often done personally. This is a responsible business approach that should not be countermanded absent a compelling public need for a different approach. For this reason, Qwest supports

[41] *Notice*, 21 FCC Rcd at 1791 ¶ 21.

[42] *Id. And see* Comments of Alexicon Telecommunications Consulting, CC Docket No. 96-115, RM-11277, filed Apr. 25, 2006 at 7 ("Alexicon EPIC Petition Comments") (stating a belief that "most carriers now notify customers of any unauthorized attempts to obtain their CPNI").

leaving the matter of customer notifications to individual businesses, barring legislative mandates.[43]

Similarly, business should be permitted to determine whether there *is* any "potential precautionary value of customer notifications *before* releasing CPNI."[44] The various fact patterns suggested in the *Notice* for prior customer notifications (*e.g.*, calling the customer's registered telephone number on the account in order to verify identity before releasing CPNI, taking additional precautionary measures if information is to be sent or delivered to other than the account-mailing address or registered e-mail address, allowing customers to request additional security measures or verifications) are not proposals devoid of costs. Carriers should be permitted to determine the business need for adopting these types of measures, which would depend on the number of customers they have, the volume of contacts, whether there are complaints and the seriousness of those complaints, and similar considerations.

Carriers should also be extended the same flexibility with respect to routine *post*-CPNI release notifications.[45] Again, the ideas reflected in the *Notice* could be extremely costly and require significant changes to carriers' operating support systems ("OSS") (*e.g.*, the ideas include a statement in a monthly bill if a customer's account has been accessed during the month, a voicemail call to cellular customers if CPNI had been released, giving customers the right to receive notice if they decide they want that). Those changes should be weighed against practical customer service and customer care considerations.

---

[43] Qwest believes that to the extent breach notifications are deemed necessary in the public interest, the decision is best left to legislative, rather than regulatory, bodies. The legislative model is usually directed to businesses that have "personally-identifiable information" in their possession, *without* regard to industry or the *particular sensitivity* of information. That is a more appropriate model than one directed to telecommunications carriers and CPNI.

[44] *Notice*, 21 FCC Rcd at 1791 ¶ 22 (emphasis added).

[45] *Id.* ¶ 23.

In theory it might sound nice to give customers the choice of receiving notifications regarding access, use and disclosure of information, either before or after releasing the information. But theory does not necessarily convert into efficient, responsive customer service. And it is highly questionable that many customers would choose the kinds of additional security measures outlined above if they were asked (or required) to pay for them.

Since there has been no convincing argument that a carrier's entire customer base should be burdened with costs and systems upgrades so that some customers can have some additional security measures that the carrier itself would not have provided absent government compulsion, the Commission should reject the proposals outlined in the *Notice*. Absent credible record evidence that carriers' existing processes and controls render the telecommunications industry peculiarly deficient with respect to their information security controls, or their customers uniquely vulnerable to information improprieties, the Commission should reserve any mandated customer notification requirements to enforcement cases where the imposition of remedial measures might be appropriate.

E. Mandated Customer-Set Passwords

The only customer-record information safeguard that EPIC proposes that even modestly aligns with its stated objective of preventing carriers from being duped into releasing information to data brokers is its proposal regarding customer-set passwords.[46] Unfortunately, EPIC's proposal is not a measured one.[47] Rather it would force customers to have passwords to interact with their carrier or make use of account information regardless of their preferences.

---

[46] MoPSC EPIC Petition Comments at 2 ("It is likely the use of consumer-set passwords will be of some value[.]").

[47] *Id.* ("While it may be a simple task to require a password when establishing service, it would be a monumental task to establish passwords for all existing telecommunications-related accounts.").

EPIC's proposal is contrary to the public interest for at least two reasons. First, it fails to accord appropriate deference to the carrier-customer business relationship. Second, it ignores the fact that passwords are not desired by all customers; in fact, for some they are a nuisance rather than a protection.

EPIC's proposal that customer-chosen passwords be mandatory is easy for it to make. It sells no services; it has no customers. It is not a business trying to be "easy-to-do-business with," friendly, efficient, and responsive to its customers in a business environment free of unnecessary costs. Qwest, unlike EPIC, is a business that has customers and wants to spend its available funds on those customers and their service needs. Qwest strives to be responsive and efficient in its relationship with its customers so that their needs are addressed quickly, conveniently, and to their satisfaction.

In pursuit of its customer service goal, Qwest already accommodates a customer's choice to use a password with respect to access and release of customer information about them. The choice is the customer's; and those who do not want a password or consider them a burden do not have to have or manage one. The model is not foolproof (again, employees with good intentions can be taken advantage of) but the option generally operates in support of those customers who want to add this additional level of protection to their account interactions.

EPIC just ignores the fact that many individuals do not want passwords, Personal Identification Numbers ("PINs") or any additional "security" layer that adds time or complexity to the completion of their task. Many individuals consider passwords to be an annoying hindrance rather than a necessary protection. After all, the customer of a telecommunications

carrier might only interact with that carrier on rare occasions.[48] Forcing a customer to have or remember a password for such isolated encounters is calculated to breed customer dissatisfaction, creating an overall negative rather than positive customer experience. Or a customer may be trying to add a fairly innocuous service, like call waiting, to an account. Declining to take the order unless there is "password proof" of identity makes little sense in such context. And there is always the persistent "problem" of forgotten or misplaced passwords. This issue often converts what should be a comfortable conversation between a business and its customer into a contentious interaction suggestive of an interrogation.

Refusing to do business with the customer unless he/she proves his/her identity through a password can sometimes improperly tilt the balance from customer privacy protection to customer annoyance and irritation. The Commission should not act to tip that balance. Rather it should defer to the business having the customer relationship the freedom to determine the appropriate balance. If the Commission decides to establish guidelines about passwords for a safe harbor, it should require no more than that carriers accommodate customers' choices to have a password.

III. QWEST'S INFORMATION SECURITY CONTROLS, INCLUDING THOSE SAFEGUARDING CPNI, BELIE THE NEED FOR ADDITIONAL CPNI RULES

Qwest safeguards its customer information, just as it does other Qwest confidential information, against improper access or disclosure. Qwest's safeguards range from sophisticated technical controls on system access, to associated processes including reviews and assessments, to employee and agent training on Qwest's ethics policies and expectations regarding the proper use of CPNI. Qwest's information security organization works diligently to support easy

[48] Verizon EPIC Petition Comments at 3 ("a customer may not need to contact his carrier for many months, and when he does have a need to talk to the carrier, may have forgotten the password he selected.").

communication between Qwest's employees and its customers, while integrating responsible customer authentication and audit tools into the relationships.

Below Qwest discusses its information controls in a general, high-level manner. All of its controls can be broken down into significantly greater detail. But it does not seem necessary to lay out all the details of a carrier's controls to demonstrate that EPIC's proposals are not in the public interest. After all, does it matter if a carrier has 20 training modules, rather than 5? Or is the important fact that training occurs? Qwest believes the latter is the case.

Moreover prudence clearly dictates that Qwest not publicly lay out in detail its information security controls or customer authentication practices. Divulging such detail would be at odds with Qwest's efforts to maintain its information integrity and security and to control the unauthorized release of CPNI to others through pretexting or otherwise.[49] And were Qwest to provide detailed information about its security controls, it would render substantial portions of the instant filing confidential, resulting in a redacted filing that would not be very useful to other commenting parties. Qwest trusts that its general, descriptive approach will be satisfactory to the Commission. Qwest would be happy to consult with the Commission, should there be something specific the Commission would like to discuss.

---

[49] *Accord* CTIA EPIC Petition Comments at 2, 3. *And see* Kim Phan EPIC Petition Comments at 9 ("Currently, the successful data broker must identify the loopholes in the security system of each carrier. Under a uniform system established by the FCC, each data broker would have a regulatory roadmap to identify any loopholes that will be overlooked by the drafters of any future rule."), 13 ("Set procedures and guidelines provide potential violators a virtual 'roadmap' to find weaknesses in a security system."). *And compare* Ohio PUC EPIC Petition Comments at 23 (cautioning "the FCC about being too specific in the technical standards it adopts" because "[w]hen the technical requirements for the implementation of a rule are uniform, the benefits of a breach of this technical standard are greatly increased" leading to an '"arms race' between the telecommunications service providers and those wishing to exploit the system").

And see id. at 4-5 and n.8 (observing that a government-industry working group might be better suited to getting specific facts regarding carriers' information security controls and vulnerabilities). *See also* Alexicon EPIC Petition Comments at 6 (supporting a working group to address CPNI security procedures, including state regulatory and legal representatives).

A. Qwest Exercises Appropriate Human Resources Controls With Respect To Employees Who Might Access And Use Customer Information

Qwest employees who interact with customers and systems that contain CPNI are well positioned to authenticate a customer's identity and to identify suspicious behavior or conversations and potential wrongdoing. Qwest appreciates the critical role employees play in overall information security and management, and accordingly acts with appropriate due diligence in its hiring and training practices.

As a first step, Qwest employees are subject to pre-employment background checks. These checks include gathering information on criminal convictions, educational background, drug testing, and work history. Depending on the specific job an employee is being hired to do, a credit check might also be required. Qwest sales and service vendors are similarly required to have their employees (Qwest's agents) undergo background checks, depending on the type of services those agents provide.

Next, Qwest employees as well as its sales and service agents receive training on a wide variety of Qwest's policies and methods. Some of these focus on employee obligations to maintain the security of CPNI and to release it only upon proper authorization. Qwest's training is provided through a number of media from paper to web-based to personal coaching; and it reflects different levels of formality from Qwest's mandated formal annual training to everyday job aids. The more formal training incorporates Qwest's annual training on its compliance program, including its Code of Conduct, the Telecommunications Act of 1996 and CPNI compliance. Job aids provide greater detail on subjects covered in the annual training and are available to service representatives through web-based material as they need them. Additionally, Qwest makes training materials similar to that described above available to its sales and service

vendors for their use in training their employees prior to those employees actually selling Qwest's products or services.

As an integral part of its overall training program, Qwest stresses not only the individual's legal obligations with respect to proper CPNI access, use and disclosure, but also the fact that in many cases Qwest has contractual obligations to maintain the confidentiality of such information. The legal admonitions regarding compliance with laws and formal commitments are married with reminders to individuals that Qwest also requires they act ethically with respect to protecting proprietary information associated with Qwest and non-Qwest entities.

While training cannot guarantee against employee or agent misconduct with respect to Qwest's assets, including CPNI, Qwest considers its training program effective and modifies that training as necessary to make it more useful to those being trained. Qwest recognizes that business processes and methods are dynamic and must keep current and relevant as business, commercial, and regulatory environments change. For this reason, Qwest works to identify gaps in its training procedures and to modify its training as appropriate to meet the requirements of the existing environment.

B. Qwest Has Reliable Systems Controls, Including For Its Customer Information Systems And Databases

1. Enterprise-Wide Activity

a. Enterprise-Wide Controls

Qwest combines proactive and reactive information security practices in its corporate ("enterprise")-wide information security program. This is the best model to manage the kinds of information security risks inherent in today's information society. While system vulnerabilities will always exist, due to the use of commercially-available information technology components

and the incentives for certain elements of society to realize illicit financial or personal gain,[50] a robust information security program focused on continuous improvement to processes and technical controls is the superior approach to protecting the confidentiality and integrity of Qwest information assets and those of its customers.[51]

Qwest employs a broad range of technical and non-technical information security controls that are supported by hardware, software, business practices and formally-defined policies and compliance processes. These controls, coupled with a strong information security organization, create a program built on industry-accepted, standard practices that provide Qwest with the requisite tools to identify, analyze and respond quickly to threats to its systems and responsibly manage any discovered vulnerabilities.

Any business using information technology on a large scale or conducting business through the Internet necessarily encounters information security risks. Qwest has fashioned a corporate-wide program to rapidly address newly-identified security vulnerabilities as one effort to mitigate such risks. The program requires formal security evaluations for new (or significantly changed) applications, technologies and products. Qwest also supports a formally-defined Cyber Incident Response Team ("CIRT") process to rapidly respond to and manage potential cybersecurity events.

Qwest believes that a quality information security organization should use products and services from a variety of vendors. Accordingly, Qwest does business with multiple vendors to ensure incorporation of different approaches and levels of coverage in the event of attacks on its

[50] *See* Ohio PUC EPIC Petition Comments at 23 ("any preventative measure can be defeated with enough persistence.").

[51] Kim Phan EPIC Petition Comments at 12 ("Whatever form of unauthorized disclosure is currently taking place, through pretexting or some other means, these methods will not last, and others are certain to be developed by wrongdoers in the future.").

information or its information technology. Qwest also consults commercial, independent and governmental resources on matters of information technology and security.

From the perspective of outreach activities, Qwest participates in a number of industry forums, standards bodies and technical and trade groups. Qwest also supports an ongoing consumer protection media campaign in an effort to educate its customers and others in the community on actions they can take to protect themselves from identity theft as well as a variety of Internet and other information security-related risks.[52]

Through its roles as a vendor, an internal supplier, a professional contributor and a community supporter, Qwest hopes to influence -- and where appropriate drive -- improvements in information security technology and practices across the industry and the technology community. Qwest can then incorporate such improvements into its own information security program in a manner that benefits Qwest's internal operations, its customer information assets, and the larger consumer and business user communities.

b. Enterprise-Wide Assessments of Controls

Qwest uses both internal and external resources to perform reviews and assessments of its overall program and technical controls, with a view to ensuring the effectiveness of its information security controls. For instance, as a part of Qwest's SOX Section 404 compliance program, Qwest performs internal assessments of its infrastructure controls that protect its underlying information technology. These internal reviews include tests of the technical controls for applications that store and provide access to CPNI. As required by SOX, Qwest's external auditing firm provides an annual attestation to the effectiveness of these controls.

[52] *See* Attachment A "ID Theft Initiative in the Spotlight Again."

There are also other examples where Qwest works cooperatively with external entities to assess Qwest's information technology and security controls. For example, for insurance underwriting purposes, Qwest works with an external firm on an annual basis to perform an overall review of Qwest's information security program, utilizing the internationally-accepted standard of information security practice as a baseline framework. Qwest also works with another firm to provide review and oversight of its Payment Card Industry ("PCI") information security compliance program, a program required for all merchants that accept and process credit card transactions.[53] Qwest utilizes the information it receives in these types of external assessments to improve its information security practices.

2. Protection from External Security Breaches

Pursuing its goal to protect its confidential information, including customer information, from inadvertent disclosure and unauthorized third-party access, Qwest uses a number of technologies to control access and release of such information. These controls include (a) perimeter control technologies such as firewalls; (b) two-factor-authentication (an authentication process incorporating an element of knowledge, such as a password, as well as an element of possession, such as a token) when access is sought through a secure dial-up or other remote entry; and (c) devices to detect and prevent network intrusions, said devices being monitored twenty-four hours a day, seven days-a-week. Qwest also employs anti-virus and anti-spam technologies at multiple computing levels including e-mail, desktop and server levels, in efforts to minimize the risk of malicious code introduction and hacking events. Qwest's multi-layered defense also includes web-content filtering and blocking, instant messaging controls and desktop

[53] *See* CTIA EPIC Petition Comments at 10.

firewalls to minimize opportunities for infection by spyware, other malicious software ("malware") and individual hacker attacks.

Qwest engineers its e-commerce environment to minimize the amount of data stored on servers exposed to the Internet. The Internet-exposed servers also employ various systems controls, to further protect the internal Qwest network and to rapidly detect any tampering or alternations to software and content. And in line with standard industry practices, Qwest encrypts confidential information in transit on the Internet, including confidential customer information.

3. Qwest Controls Access to its Customer Information Systems and Has Reasonable Audit Trails in Place to Monitor Such Access

a. Only Employees that Need CPNI Access Have Access

Qwest permits access to its systems and databases that house CPNI in those cases where there is a need for such access as part of an assigned job function. Qwest employees that meet this requirement are generally those who have some type of customer contact responsibilities (such as business offices, customer-care centers, repair, executive complaints and finance/billing), along with limited numbers of individuals with closely-related support functions, such as regulatory compliance, security, legal and audit.

Requests that system access be extended to non-employees, such as agents, require that a Qwest management employee sponsor the agent and make a formal request for access. The Qwest-sponsoring employee is expected to provide oversight and supervision of the agent's use of Qwest's systems and data throughout the term of the business relationship.

Just as Qwest has processes for granting systems access, it has formally-defined and auditable methods for quickly taking access away when the business relationship terminates.

b. Qwest Has Reasonable System Controls Associated with CPNI Databases

In addition to general information security controls and employee training, Qwest uses a variety of software and technology tools to detect and prevent the improper access or disclosure of CPNI. These tools generally fall into three categories: (1) controls Qwest uses to protect its information from external security breaches, *e.g.*, hacking; (2) controls Qwest uses that provide access restrictions, audit trails and other measures to prevent internal misuse by employees or agents; and (3) controls in the nature of directives admonishing its employees to act lawfully and ethically and to report unlawful or unethical behavior, supplemented by investigations in the event of alleged wrongdoing. The first category was addressed above with respect to enterprise-level controls. Below Qwest discusses the technologies associated with user access controls, auditing capabilities, and investigations of wrongdoing.

With respect to the second category, as previously described, Qwest restricts access to databases that contain customer information to those persons with a business reason for such access. It also uses audit trails (sometimes called "logs") at both the application and computer operating system levels to collect information about access to data by both application users and system administrators (the latter sometimes called "privileged users").

Qwest retail sales locations and data centers are protected by physical security controls as well that act to safeguard access to and improper disclosure of Qwest confidential information, including CPNI. Qwest's computers that store CPNI, and are accessible in on-site situations, have been recently updated to further reduce the amount of CPNI stored on-site. Qwest also inventories backup tapes from applications that may contain CPNI and stores the tapes in physically secured locations. The backup tapes use a proprietary format so that the tapes are not readily viewable without Qwest application software or specific computing capabilities.

c. Controls Requiring Lawful and Ethical Employee Conduct, Reporting of Improper Conduct and Investigation of Alleged Wrongful Conduct

With regard to the third management tool referenced above (employee accountability for right and wrong actions), Qwest has an extensive, high-quality Corporate Ethics and Compliance program. As part of that program, Qwest's Code of Conduct and related Corporate Policies require employees to act lawfully and ethically. Supervising managers in business offices and similar retail environments are expected to review and monitor the activities of their work force as a part of their supervisory responsibilities.

Qwest's Code of Conduct and related Corporate Policies requires employees to report illegal or inappropriate conduct whether committed by employees, agents, or third parties. Qwest employees are reminded of their obligations to engage in ethical business practices and report any suspected wrongdoing through Qwest's internal and external websites, mandatory training programs and various other types of communications such as posters and notices. Qwest fields complaints about inappropriate conduct through a variety of venues, including a twenty-four hour, seven day-a-week hot line and an Advice Line e-mail box; the Security and Fraud departments; Qwest's Customer Advocacy Group; individual employees; and e-mails sent to Qwest's Chief Executive Officer. Reports may be made to the hot line anonymously; and when wrongdoing is alleged, Qwest investigates the matter as appropriate.

As is appropriate to any particular investigation of alleged wrongdoing, Qwest may employ forensics technologies and other monitoring and data-searching mechanisms to investigate and further monitor employee actions to gather evidence and assure the protection of CPNI. These mechanisms include reviewing and analyzing the information made available by the logs built into Qwest's applications and systems.

At the conclusion of each investigation, Qwest determines the proper response and acts accordingly, including taking disciplinary measures that might range from additional coaching or warnings to dismissal. It also considers and implements remedial measures as appropriate. Qwest also cooperates with law enforcement in the prosecution of illegal conduct as required or permitted by law.

C. Customer Authentication Controls

1. General Authentication Practices

Qwest trains its customer service representatives to verify the identity of the calling party before discussing or disclosing CPNI. The verification process utilizes a range of questions and information points, where the responsive information would likely be known by an individual account holder and those authorized to act on behalf of the account holder.[54] Depending on the facts of any particular call, Qwest's service representative will ask for a password, or social security number ("SSN") information,[55] or information that can be found only on a customer's bill, or other kinds of information that Qwest might verify against its records, such as where a customer might be reachable during the day or his/her place of employment.

When Qwest interacts with customers in contexts other than over the telephone, Qwest may seek additional or different kinds of verification. For example, PINs or "secret question/answer" elements[56] might be used in the context of Voice Response Units ("VRU"), on-

[54] For example, the Commission's slamming rules confirm that there are those beyond the named account holder that could be authorized to make decisions about an account. *See* 47 C.F.R. § 64.1100(h) (defining the word "subscriber" more broadly than account holder).

[55] In a different context, the Commission had identified the SSN as an appropriate verifier of identity. *See* 47 C.F.R. § 64.1120(c)(3) (slamming rule).

[56] *See Notice*, 21 FCC Rcd at 1789 ¶ 15. An example of a "secret question/answer" would be where the account holder would say: My question is "What was your address in 1993?" and then would provide the right answer "xxxx." Individuals might find this kind of screening device more accommodating than passwords in their specific case.

line activity, or retail site operations. Customers at retail locations are expected to show Qwest employees at least one form of picture identification, in addition to other verification elements, before an employee will discuss or release CPNI. In those cases where a customer is at a retail Qwest site and wants account information but cannot remember the password (if the account is so restricted) or asks for a duplicate bill, the customer is referred to Qwest's business office to get the information they seek.

Every month, Qwest assesses its service representatives' compliance with customer-authentication policies through a "quality monitoring" model that incorporates more formal and less formal components. The more formal monitoring is done by a Quality Assurance Group that scores each representative on a variety of criteria, one of which is "verified caller authorization." The less formal monitoring is done by Qwest supervisors, who are expected to observe calls and review any issues that arise from their observations with their team members. Inadequate customer authentication might be such an issue.

Qwest has been reviewing its training materials regarding customer authentication. For example, it has modified its CPNI training to highlight the potential problems of data brokers and pretexting and re-emphasize the critical role of proper customer authentication. Qwest will continue to make changes in its training so that the training remains relevant, clear and topical.

2. On-Line Account Creation and Access

Currently, a Qwest customer cannot *establish* service through an on-line account, although he/she may utilize the website to send an initial order requesting to establish service. Qwest then processes the order through normal channels. In due course, the customer receives his/her first bill at the address they provided with the initial order.

Once the first billing cycle completes, the individual may choose to establish an on-line account with Qwest. That process begins by creating an on-line profile.[57] An on-line profile is created by providing certain widely-required information (such as name, billing address, other authorized parties, and similar information) along with specific individual information selected to authenticate the requestor; affirmatively populating a field certifying that the person creating the profile is authorized to make changes to the account; creating a unique user name and password for the profile; and selecting a security question and answer (a "secret question").[58]

Once an individual has created an on-line profile, the customer may access the account by providing the correct name and password. If a customer forgets the password *and* there is a security question/answer on file,[59] Qwest will direct the customer to a page where a user name and an e-mail address can be entered. If both pieces of information correspond to that in Qwest's systems, the customer will be directed to a security question as a screening device. If the customer answers the security question correctly, Qwest will provide by e-mail a temporary password to the customer at the e-mail address on file.[60] The customer will then be required to take some additional measures to create a new password to replace the temporary one.

IV. SAFE HARBOR GUIDELINES

As indicated throughout this filing, Qwest appreciates that the Commission might want to re-emphasize the importance of carriers protecting CPNI against unauthorized access, use and

---

[57] Qwest wireless customers may obtain general plan information on-line, such as information about minutes used or available, without first establishing an "on-line account." These customers must establish an on-line profile to access other information such as billing or call details.

[58] *See* note 56, *supra*.

[59] Qwest recently instituted the security question/answer process. Some older customer profiles were created without them. Qwest provides an option on its website for customers with older profiles to update their account information should they wish to.

[60] *See* CTIA EPIC Petition Comments at 18.

disclosure. But formal amendments to the CPNI rules are not necessary to accomplish that goal. The existing CPNI rules, coupled with carriers' statutory duty to protect customer proprietary information (47 U.S.C. § 222(a)), is sufficient government articulation of carriers' obligations. Carriers that violate the rules or the statutory admonition would be likely targets of Commission enforcement action.

But should the Commission become wedded to the position that some rule changes are necessary, those changes can be modest. The Commission could either act immediately to promulgate additional CPNI safeguard rules or might wait to benefit from recommendations from some type of industry/government working group.[61] But the goal should be to frame guidelines which, if incorporated into carriers' business practices, would form a safe harbor from enforcement action, along the lines of the safe harbor incorporated in the Commission's TCPA rules.[62]

While an industry group might recommend a broader set of guidelines, or frame proposed guidelines differently, Qwest believes the following items could fairly be included safe harbor guidelines adopted by the Commission:

- An annual filing by a carrier of its CPNI Certifying Officer Certificate and supporting information;

---

[61] *See* note 49, *supra*. *And compare* Kim Phan EPIC Petition Comments at 14 ("The telecommunications industry leaders could work together to address this problem and develop the best and most uniform reporting system rather than having the FCC craft one through government intervention."). Phan supports government reporting of CPNI breaches, which Qwest does not necessarily support. But the concept of the industry developing "best practices" is not unheard of. This model was utilized with respect to "cramming." *See* News Release, dated July 22, 1998, FCC and Industry Announce Best Practices Guidelines to Protect Consumers from Cramming.

[62] *See* pp. 7-8 and note 14, *supra. And see In the Matter of Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, Report and Order, 18 FCC Rcd 14014, 14040 ¶ 38 ("A seller . . . that has made a good faith effort [to comply with the law] should not be liable for violations that result from an error.").

- A short, non-confidential descriptive statement, in its Officer Certificate or otherwise, of its current hiring practices and controls;

- A short, non-confidential statement and general description, in its Officer Certificate or otherwise, that a carrier has written methods and procedures regarding customer authentication and an outline of those methods;

- A short, non-confidential statement and general description, in its Officer Certificate or otherwise, that a carrier has reasonable information security controls, including audit capabilities, that incorporate administrative, technical and physical safeguards, appropriate to a carrier's size and complexity, the nature and scope of activity and the sensitivity of the information at issue;[63]

- A carrier commitment, in its Officer Certificate or otherwise, that it will accommodate a customer's request for a password/PIN/secret question and answer on an account, whether the account is an online account or one more traditionally created and accessed over the telephone; and

- A commitment from a carrier, in its Officer Certificate or otherwise, to retain records for only so long as they support a legitimate business purpose.

There may be other elements that should be included in a safe harbor. Qwest will review the filed comments to determine whether it can support additions to its proposal. In any event, a safe harbor approach is a sound one to pursue. It establishes regulatory expectations but still provides flexibility for those subject to the regulations; and it accommodates the critical fact that information security practices are dynamic by nature and need to remain so to accomplish their fundamental objective.

V. CONCLUSION

The Commission should reject EPIC's proposals with respect to encryption of data in storage, "track everything" audit trails, data retention and breach notifications. Nor should the Commission adopt a "notify all customers of all CPNI access, use and disclosures" rule. All these proposals would saddle carriers with millions of dollars of administrative and operational

[63] CTIA EPIC Petition Comments at 9-10 (discussing the FTC's Gramm-Leach-Bliley "Safeguard Rules" and observing that they "are very flexible and do not dictate the design of the security management program; indeed, they are notable for their simplicity.").

costs at a time when their investments should be focused on innovative products and services to provide greater choices for consumers in the marketplace.

The Commission should consider announcing that it expects carriers to honor requests for passwords, at least to the extent they are technically capable of doing so. Formal rules should not be necessary, since a Commission pronouncement would be the equivalent of a warning that failure to act in a certain manner could well be found an unreasonable practice under 47 U.S.C. § 201(b).

Finally, while damning those that seek to defraud carriers, the Commission should acknowledge the laudatory efforts of carriers across the county to craft and maintain robust, reasonable and most-often effective information security controls. Those controls are technical and educational, investigative and responsible. There is no evidence in the record to suggest otherwise, and Qwest believes none will be forthcoming.

For all the reasons stated above, Qwest believes the best course of action would be for the Commission to terminate the current proceeding with a finding that the overwhelming majority of carriers already have reasonable security tools and controls imbedded in their operations and

that nothing more is required at this time. Alternatively, a modestly crafted, commercially reasonable and achievable safe harbor could be crafted in an effort to re-emphasize the serious obligations imposed on carriers to protect customer proprietary information.

Respectfully submitted,

QWEST COMMUNICATIONS
INTERNATIONAL INC.

By: Kathryn Marie Krause
Craig J. Brown
Kathryn Marie Krause
Suite 950
607 14th Street, N.W.
Washington, DC 20005
303-383-6651

April 28, 2006

ATTACHMENT A

ID THEFT INITIATIVE IN THE SPOTLIGHT AGAIN

Qwest's Teen Identity Theft Education Program is striking a chord with teens and the national media. Melodi Gates, Qwest director of risk management/information security, appeared yesterday, April 25th on the Montel Williams show to discuss Qwest's program and provide advice about how Montel's viewers can protect themselves from becoming victims of identity theft.

"Qwest is leading the charge in teen identity awareness outreach and the national media is paying attention," said Melodi. "The Qwest Teen Identity Theft Program's goal is to arm teens and their parents with information about how to protect themselves, in the hope to help reduce the number of incidences of identity theft overall."

As part of Qwest's Spirit of Service, Qwest wants to help educate its customers and all consumers on the growing epidemic of identity theft crimes. To help educate the teen audience about identity theft, Qwest is hosting a speaking series on "Teen Identity Theft Awareness" with Zach Friesen, a college student who was a teen identity theft victim. Friesen speaks at various high schools throughout the Qwest 14-state region and talks to about identity theft and how to protect yourself. Qwest also has developed a teen identity theft resource guide on its web site www.incredibleinternet.com.

The Montel Show appearance for Melodi is the second national broadcast exposure for the Qwest Identity Theft program this year. On Jan. 16, Zach and Melodi were interviewed by CBS consumer reporter Susan Koeppen on "The Early Show." In addition to the national networks, Qwest's teen identity theft program has been featured in major print publication including *The Christian Science Monitor, The Chicago Tribune* and *The Washington Times* as well as numerous publications throughout the 14-state region. More than 11 million people nationwide have been exposed to Qwest and its initiative since the beginning of 2006. To learn more about the Qwest program and tips to protect yourself and your teen from identity theft please visit www.incredibleinternet.com

CERTIFICATE OF SERVICE

I, Richard Grozier, do hereby certify that I have caused the foregoing **COMMENTS OF QWEST COMMUNICATIONS INTERNATIONAL INC. TO ADDITIONAL CUSTOMER PROPRIETARY NETWORK INFORMATION RULEMAKING** to be: 1) filed with the FCC via its Electronic Comment Filing System in CC Docket No. 96-115; 2) served, via e-mail on Ms. Janice Myles, Competition Policy Division, Wireline Competition Bureau at janice.myles@fcc.gov; and 3) served, via e-mail on the FCC's duplicating contractor Best Copy and Printing, Inc. at fcc@bcpiweb.com.

/s/ Richard Grozier
Richard Grozier

April 27, 2006