

Donna Epps
Vice President
Federal Regulatory



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

Phone 202 515-2527
Fax 202 336-7922
donna.m.epps@verizon.com

March 3, 2008

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

Re: **Filing of Customer Proprietary Network Information (CPNI) Compliance Certifications, EB Docket No. 06-36 and Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services , CC Docket No. 96-115**

Dear Ms. Dortch:

In accordance with the April 2, 2007 *Report and Order and Further Notice of Proposed Rulemaking* (EPIC CPNI Order),¹ Verizon hereby provides copies of its 2007 certifications of compliance with the rules for protecting customer proprietary network information, pursuant to 47 C.F.R. §64.2009(e).

Sincerely,

A handwritten signature in black ink that reads "Donna Epps".

Attachments

cc: Marcy Greene
Best Copy and Printing

¹ *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, CC Docket No. 96-115; WC Docket No. 04-36, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) ("EPIC CPNI Order").

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date filed: March 1, 2008

Name of companies covered by this certification: Verizon Telecom (see attachment)

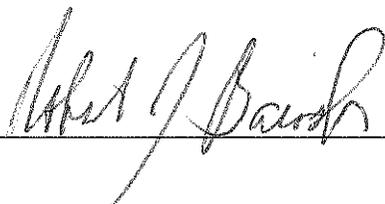
Name of signatory: Robert J. Barish

Title of signatory: Senior Vice President and Chief Financial Officer

I, Robert J. Barish, certify that I am Senior Vice President and Chief Financial Officer of Verizon Telecom, a unit of Verizon Communications Inc. that markets the telecommunications and interconnected VoIP services of the carriers listed on the attachment to residential and small business customers. I further certify, acting as an agent of Verizon Telecom, that I have personal knowledge that Verizon Telecom has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how Verizon Telecom's procedures ensure that it is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules, including an explanation of actions taken against data brokers and a summary of customer complaints received in 2007 concerning the unauthorized release of CPNI.

Signed: _____

A handwritten signature in cursive script, appearing to read "Robert J. Barish", is written over a horizontal line.

VERIZON TELECOM CARRIERS

Entity Name

Verizon New England Inc.
Verizon New York Inc.
Verizon Washington DC Inc.
Verizon Delaware LLC
Verizon Maryland Inc.
Verizon New Jersey Inc.
Verizon Pennsylvania Inc.
Verizon Virginia Inc.
Verizon West Virginia Inc.
Verizon California Inc.
Verizon Florida Inc.
Verizon North Inc.
Verizon Northwest Inc.
Verizon West Coast Inc.
Verizon South Inc.
GTE Southwest Inc. d/b/a Verizon Southwest
Contel of the South Inc. d/b/a Verizon Mid-States
Verizon Select Services Inc.
Verizon Hawaii International Inc.
NYNEX Long Distance Company d/b/a Verizon Enterprise Solutions
Bell Atlantic Communications Inc. d/b/a Verizon Long Distance
Verizon Avenue Corp. d/b/a Verizon Enhanced Communities
MCImetro Access Transmission Services LLC d/b/a Verizon Access Transmission Services
MCImetro Access Transmission Services of Virginia, Inc. d/b/a Verizon Access Transmission
Services of Virginia
MCImetro Access Transmission Services of Massachusetts, Inc. d/b/a Verizon Access
Transmission Services of Massachusetts

Verizon Telecom 2007 CPNI Statement of Compliance

In order to promote ongoing compliance with Section 222 of the Communications Act of 1934 (the “Act”) and the Commission’s implementing rules (the “rules”), Verizon Telecom (“VZT”)¹ maintains a CPNI compliance program. The program is designed to ensure that the business entities supported by VZT that are subject to the Commission’s CPNI requirements understand the rules and have taken appropriate measures to comply. The program is structured around a Compliance Manager function in each of these business units. These managers are responsible for overseeing CPNI compliance, including the implementation of appropriate controls, within their respective organizations. In this way, each organization is charged with ensuring that its employees are appropriately trained to comply with the CPNI rules. The Legal Department and the Regulatory, Privacy and Compliance organizations, ensure that the Compliance Managers have been given clear direction on their compliance responsibilities and the details and proper interpretations of the Commission’s CPNI rules. VZT employees in the Regulatory, Privacy, Compliance and Legal Departments work with the Compliance Managers on a regular basis to review issues that may arise and to provide advice and guidance.

The Compliance Manager responsibilities include:

- Ensuring the ongoing availability and effectiveness of department-specific methods and procedures, and job aids for supervisory and non-supervisory personnel.
- Ongoing training programs for supervisory and non-supervisory personnel, including introductory training for employees that are newly entering the company or the department. The Compliance Manager is also charged with implementing job appropriate tracking mechanisms, such as employee sign-offs and training session rosters, to ensure that any training provided can be subsequently verified.
- Maintaining awareness within the department of the importance and necessity of complying with the CPNI rules. This could include CPNI notices and periodic awareness training sessions. All employees are specifically advised that violation of VZT CPNI guidelines may result in disciplinary action, up to and including dismissal.
- Performing internal operational reviews as appropriate to evaluate the effectiveness of departmental methods and procedures and compliance guidelines.
- Managing and controlling access to domestic and international CPNI databases to ensure that CPNI is disclosed only as permitted under the Commission’s rules.

¹Verizon Telecom is a unit of Verizon Communications Inc. that markets the telecommunications and interconnected VoIP services of the carriers listed on the attachment entitled “Verizon Telecom Carriers” to residential and small business customers.

Section 64.2005 Use of Customer Proprietary Network Information Without Customer Approval

Verizon Telecom is a provider of local and long distance telecommunications and interconnected VoIP service to residential and small business customers. In the absence of customer approval, VZT's training, operating procedures and disciplinary processes are designed to ensure that CPNI is only used to provide or market its service offerings to its customers within the categories of services to which the customer already subscribes (subject to the exceptions listed in 47 U.S.C. §222(d) and the exemptions in this subpart.) In addition, in the absence of customer approval (and subject to the above exemptions in this subpart), VZT's procedures are designed to ensure that CPNI will be shared only with affiliates that provide services in the categories to which the customer already subscribes. VZT's training makes clear that it does not use, disclose, or permit access to CPNI for marketing purposes, other than pursuant to the "total service approach" authorized by section 64.2005(a) or for the limited purposes set forth in section 64.2005(c), unless it has customer approval to do so pursuant to the procedures described below in section 64.2007 and 64.2008. VZT does not share CPNI with an affiliate under the "total service approach" until its Information Technology group has reconciled its customer list against that of its affiliate to ensure that each customer is served by both companies. VZT does not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers.

Section 64.2007: Approval Required for Use of Customer Proprietary Network Information

Verizon Telecom obtains opt-out approval from its customers to use CPNI and to disclose CPNI to its affiliated carriers named in the attachment, as well as to its Verizon Wireless and Verizon Business affiliates (collectively "Affiliates"), and their respective agents, for the purpose of marketing the communications-related services of those affiliated carriers. VZT's training and operating procedures are designed to ensure that when VZT obtains customer consent to use CPNI for marketing, it does so through written, oral, or electronic methods. Customer requests to opt out received via the 800 number provided in VZT's opt-out notice, or in written or electronic form, are maintained in an opt-out database that is used to ensure that the customer's CPNI is properly restricted.

When VZT relies on oral approval, appropriate mechanisms are in place to demonstrate that the customer has been properly notified and that consent has been obtained. Customer service representatives obtaining oral consent to the one-time use of CPNI are trained to request the customer's consent to access the customer's records when appropriate, and to record that consent. VZT maintains records of opt-out notices that it sends to customers, and any opt-out requests that it obtains from its customers, whether oral, written or electronic, for at least one year. Such records may be kept in paper or electronic format.

VZT's policy is not to use or disclose CPNI for purposes other than permitted under 47 U.S.C. §222 and the Commission's implementing rules. VZT does not disclose CPNI to third parties for the purpose of marketing any non-communications related products or services.

Section 64.2008: Notice Required for Use of Customer Proprietary Network Information

In 2007, VZT provided opt-out notices consistent with the pre- and post- December 8, 2007 requirements of this subsection. VZT provides written opt-out notice to its customers when they sign up for service and on a biennial basis thereafter consistent with the requirements of this subsection.

Effective December 8, 2007, the notice includes the following content: It states that CPNI is information relating to the quantity, technical configuration, type, destination, location, and amount of use of telecommunications services purchased, and related local and toll billing information that is made available to VZT solely by virtue of the customer's relationship with VZT. The notice advises customers that their CPNI may be shared with VZT's affiliates and agents to offer them a wide range of telecommunications services that may be different from those they already buy from the VZT family of companies; that the customer has the right to opt out of such use and sharing at any time; and that opting out will not affect provisioning of services to which the customer subscribes. The notice provides customers with a toll-free number to call for CPNI opt-out purposes. This toll free service is available 24 hours a day, seven (7) days a week on a year-round basis. Customers are advised that they can opt out at any time and that their opt-out status remains in place unless the customer contacts VZT to change it.

VZT adheres to a minimum 30-day waiting period when providing opt-out notice and allows five additional days for mailing before using CPNI under opt-out. Customer requests to opt out received via the 800 number provided in VZT's opt-out notice, or in written or electronic form, are maintained in an opt-out database that is used to ensure their CPNI is properly restricted. VZT uses oral notice to obtain customer consent to use CPNI for the duration of a customer call. The oral notice complies with the requirements of this section. VZT provides opt-out notification via e-mail to a very small portion of its customer base. These notices comply with the requirements of this section.

Section 64.2009: Safeguards Required for Use of Customer Proprietary Network Information

VZT maintains a standard operating procedure that enables marketing and sales personnel to establish the status of a customer's CPNI approval prior to the use of CPNI. Operational procedures and systems are in place that identify and maintain a record of marketing and sales campaigns that utilize CPNI, including records of associated disclosure to or access by affiliates and agents. An employee who proposes an outbound marketing campaign that involves the use of CPNI is required to obtain approval from that employee's supervisor before initiating that campaign, and to submit a list request form which describes the campaign, the specific CPNI that is to be used in the campaign, who is requesting the information, what products and services are to be offered as part of the campaign, and the date of disclosure.

VZT maintains records of its sales and marketing campaigns and supervisory reviews for a minimum of one year. Campaign records include a description of the campaign, the CPNI that was used in the campaign, and what products or services were offered as part of the campaign. VZT also maintains a compliance program that includes an employee training program component within each business unit. VZT's training program informs all employees, including sales and marketing personnel, about the CPNI rules and that failure to follow the CPNI rules can be grounds for disciplinary action, up to and including dismissal. VZT also trains its employees who are responsible for seeking, tracking, and maintaining records of consent from its customers. In addition, VZT agents who have access to confidential information are required to complete training in the protection of CPNI.

VZT provides each customer with a toll-free number to call to establish CPNI opt-out status. This toll free number is available 24 hours a day, seven (7) days a week on a year-round basis. VZT has in place a process to provide written notice to the Commission within five business days should a failure of this opt-out mechanism occur that is more than an anomaly. The written notice meets the content requirements identified in this subsection.

This statement of compliance is preceded by a certificate signed by an officer of Verizon Telecom, pursuant to section 64.2009(e). An explanation of actions taken against data brokers and summary of customer complaints involving instances of the unauthorized release of CPNI is attached below.

Section 64.2010: Safeguards on the disclosure of customer proprietary network information

VZT has taken reasonable procedural and technological measures to discover and protect against unauthorized CPNI access. VZT's operational procedures require that customers or their representatives be properly authenticated, as required by this section, before they are given access to CPNI. VZT does not disclose call detail CPNI on inbound calls, except as permitted under the business customer exception noted in subsection (g). VZT will only discuss call detail over the phone with a customer during a customer-initiated call if that customer is able to provide the specific call detail to be discussed without assistance from the service representative.

VZT's online process does not rely on readily available biographical or account information to authenticate a customer. And once authenticated, a customer may only obtain online access to CPNI by providing a password. In the event of a lost or forgotten password, VZT's back-up authentication process does not prompt the customer for readily available biographical or account information. If a customer cannot provide a password or satisfy the back-up authentication process, that customer is required to establish a new password in accordance with the requirements of subsection (e) above.

VZT's operating procedures require a valid photo ID matching the customer's account information before disclosing CPNI at a retail location and confirmation that the customer provided a valid photo ID is noted in the record of the customer transaction.

VZT has established procedures to immediately trigger notification to the affected customer when a password, customer back-up authentication response, online account, or address of record is created or changed, except at service initiation. Such notices do not reveal the changed information and are sent to a customer address of record (as defined by subsection 64.2003(b) or to the telephone number of record (as defined in subsection 64.2003(p)).

Section 64.2011: Notification of customer proprietary network information security breaches

VZT has implemented procedures to notify law enforcement, and subsequently customers, of CPNI breaches (defined in subsection 64.2011(e)), as required by this section. Internal procedures direct information about possible CPNI breaches to an established CPNI email address routed directly to Security. The information is then made available to a team including Verizon security, privacy and legal groups. Such possible breaches are then investigated and handled according to the requirements of this section.

In particular, VZT procedures require that the United States Secret Service (“USSS”) and the Federal Bureau of Investigation (“FBI”) be notified of a CPNI breach through the central reporting facility required under subsection 64.2011(b) as soon as practicable, and in no event more than seven business days after VZT reasonably determines that the breach has occurred. Customers and the public will not be notified of a CPNI breach during the seven business days after notification has been given to the USSS and FBI, except as permitted under subsections 64.2011(b)(2) in case of extraordinarily urgent need, to avoid immediate and irreparable harm, and after consulting and cooperating with the relevant investigative agency to minimize any adverse effects of the customer notification. If the relevant investigating agency directs VZT in writing not to disclose to or notify customers or the public of a CPNI breach because such disclosure or notice would impede or compromise an ongoing or potential criminal investigation or national security, as provided by subsection 64.2011(b)(3), VZT will further delay notifying or disclosing the CPNI breach to customers and the public. After VZT has completed the process of notifying law enforcement of a CPNI breach, including the required periods of delay noted above, VZT procedures require that the affected customer be notified of the breach. Records of CPNI breaches, notifications to the USSS and FBI pursuant to subsection 64.2011(b), and notifications to customers, will be maintained for at least two years. Those records will include, if available, the dates the CPNI breach was discovered, the dates notifications were made, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Information Concerning Data Brokers and Complaints of Unauthorized Disclosure

Explanation of Actions Against Data Brokers

In 2007, VZT took the following actions, as defined by the Commission, against data brokers:

In December 2006, Verizon and Verizon Wireless together filed suit against several corporate defendants and certain of their officers to stop them from unlawfully accessing confidential customer information via online accounts. The lawsuit, Cellco Partnership d/b/a Verizon Wireless, et al., v. Worldwide Investigations Inc., et al. (Civ. Action. No. 06-CV-05792, filed D. N.J.), alleged that defendants used customer telephone numbers and confidential customer information required for authentication and account access, in order to establish unauthorized online accounts, and/or to access existing accounts. During 2007, the suit was amended to add other defendants. All defendants agreed to consent injunctions banning unlawful pretexting behavior, and to settle with Verizon and Verizon Wireless. Settlement proceeds from the lawsuit are being donated to charities designated by Verizon and Verizon Wireless.

Information of VZT about Processes Used by Pretexters to Access CPNI and VZT Actions in Response to Protect CPNI

VZT also learned in 2007 that pretexters in the past had called customer service representatives and pretended to be customers or company employees so they could obtain access to confidential account information. In the past, some data brokers also appear to have obtained confidential authenticating information, such as social security numbers or date of birth, from their clients who were asking the pretexters to obtain CPNI, or from other external online sources.

Summary of the Number of Customer Complaints in 2007 Concerning Unauthorized Release of CPNI

VZT's summary of 2007 CPNI complaints by category appears below. Because the requirement to report such complaints did not become effective until December 8, 2007, during most of 2007, VZT's recordkeeping systems tracked complaints only in a category that included any unauthorized access, use or disclosure of proprietary information. A review of the allegations falling into this category revealed a total of 16 substantiated complaints involving CPNI. The 16 complaints break out as follows (one substantiated complaint fell within two categories):

Number of complaints involving improper access by employees: 10

Number of complaints involving improper disclosure to unauthorized individuals: 6

Number of complaints involving improper online access by unauthorized individuals: 1

Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date filed: March 1, 2008

Name of companies covered by this certification: Verizon Business (see attachment)

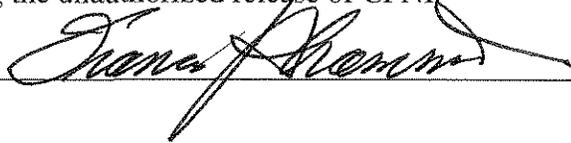
Name of signatory: Francis J. Shammo

Title of signatory: Senior Vice President and Chief Financial Officer

I, Francis J. Shammo, Senior Vice President and Chief Financial Officer of Verizon Business, hereby certify as follows:

1. Verizon Business is a unit of Verizon Communications Inc. which markets the telecommunications and interconnected VoIP services of the carriers listed on the attachment to enterprise business and governmental customers.
2. I have personal knowledge that Verizon Business has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*
3. Attached to this certification is an accompanying statement explaining how Verizon Business's procedures ensure that it is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules, and an explanation of actions, if any, taken against data brokers and a summary of customer complaints received in 2007 concerning the unauthorized release of CPNI.

Signed: _____



VERIZON BUSINESS CARRIERS

Long Distance and Interconnected VoIP Providers

MCI Communications Services, Inc. d/b/a Verizon Business Services
Verizon Select Services Inc.

Local Service Providers

Verizon Delaware Inc.
Verizon Washington, DC Inc.
Verizon Maryland Inc.
Verizon New England Inc.
Verizon New Jersey Inc.
Verizon New York Inc.
Verizon Pennsylvania Inc.
Verizon Virginia Inc.
Verizon West Virginia Inc.
Verizon California Inc.
Verizon Florida Inc.
Verizon North Inc.
Verizon Northwest Inc.
Verizon South Inc.
Verizon West Coast Inc.
GTE Southwest Inc. d/b/a Verizon Southwest
Contel of the South, Inc. d/b/a Verizon Mid - States
MCImetro Access Transmission Services LLC d/b/a Verizon Access Transmission
Services
MCImetro Access Transmission Services of Virginia, Inc. d/b/a Verizon Access
Transmission Services of Virginia
MCImetro Access Transmission Services of Massachusetts, Inc. d/b/a Verizon Access
Transmission Services of Massachusetts

Verizon Business 2007 CPNI Statement of Compliance

Rule § 64.2005 Use of Customer Proprietary Network Information Without Customer Approval

Verizon Business¹ is a provider of local and long distance telecommunications and interconnected VoIP services to enterprise business and governmental customers. It does not use, disclose, or permit access to CPNI of these customers, other than as permitted under the total service approach reflected in subsection 64.2005(a), Title 47 of the Code of Federal Regulations, or for the limited purposes specified under 47 C.F.R. subsection 64.2005(c) or under subsection 222(d) of the Communications Act of 1934, unless it has opt-in customer approval to do so pursuant to the notice procedures described below regarding sections 64.2007 and 64.2008. It does not use, disclose, or permit access to CPNI to identify or track customers that call competing service providers.

Rule § 64.2007 Approval Required for Use of Customer Proprietary Network Information

Verizon Business seeks opt-in approval from its customers to use CPNI and to disclose CPNI to its affiliated carriers named in the attachment titled "Verizon Business Carriers," as well as Verizon Wireless and its affiliates (collectively "Affiliates"), and their respective agents and partners, for the purpose of marketing the communications-related services of all of those affiliated carriers. When obtained, that approval is recorded in Verizon Business systems. Pursuant to section 64.2007(a)(2), customer approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval. Verizon Business sales, service and marketing personnel are trained to use those systems to verify customer approval before using or disclosing CPNI for a purpose requiring approval (e.g., outside of the total service approach). Pursuant to section 64.2007(a)(3), Verizon Business maintains records of customer approvals for at least one year.

Rule § 64.2008 Notice Required for Use of Customer Proprietary Network Information

As explained above, Verizon Business seeks opt-in approval from customers for the purpose of marketing the communications-related services of its Affiliates. Individual notices to business customers are provided when soliciting approval to use, disclose or permit access to customers' CPNI. The notice informs the customers of their rights to restrict use, disclosure, and access to their CPNI, and provides sufficient information to

¹ For purposes of this document, Verizon Business means the Verizon business carrier that markets, directly or through agents, telecommunications and interconnected VoIP services to enterprise business and governmental customers. The carriers are listed on the attachment titled "Verizon Business Carriers."

enable the customers to make informed decisions as to whether to permit Verizon Business to use, disclose, or permit access to, the customers' CPNI. As set forth below, the contents of the notice comply with both the general requirements for notices and the specific requirements for opt-in notices in section 64.2008. Verizon Business maintains records of these notifications for at least one year.

The notice includes the following content (although the specific language used to convey it may vary). The notice states that carriers have a duty, and the customer has a right, under federal law to protect the confidentiality of customer's CPNI. The notice states that CPNI includes information relating to the quantity, technical configuration, type, destination, location, and amount of use of the telecommunications² services the customer purchases from the Affiliates, as well as related local and toll billing information, made available to the Affiliates solely by virtue of customer's relationship with the Affiliates. The notice seeks consent to share customer CPNI and other confidential information among the Affiliates, and with agents and partners, so that all may use it to offer customer the full range of products and services offered by the Affiliates. The notice states that customer grants consent by signing but that the customer has the right to refuse consent by sending notice of that refusal in writing to cpni-notices@verizonwireless.com and cpni-notices@verizonbusiness.com. Finally the notice states that the customer's decision to consent or refuse consent will remain valid until the customer otherwise advises Verizon Business, and in either case, will not affect the provision of service to customer. The notice is presented in at least 10-point font, and may be provided to the customer as a separate document, or in the customer's service agreement (located near the customer's signature). Except in the State of Arizona where carriers are required to provide notice in Spanish as well as English, no portion of the notice is translated into another language. The notice does not include any statement attempting to encourage a customer to freeze third-party access to CPNI. As noted above, Verizon Business does not seek opt-out CPNI approvals.

Rule § 64.2009 Safeguards Required for Use of Customer Proprietary Network Information

Verizon Business has implemented systems by which the status of a customer's CPNI approval can be clearly established prior to the use or disclosure of CPNI. When a customer CPNI approval is received, it is recorded in Verizon Business systems, including the date. If the customer withdraws that approval, the systems are updated to reflect the withdrawal. Sales, service and marketing personnel can reference the systems whenever needed to determine a customer's current CPNI approval status.

Consistent with the requirements of section 64.2009(b), Verizon Business trains sales, service and marketing personnel about the CPNI rules and that the failure to follow them can be the grounds for disciplinary action, up to and including dismissal. New training, including the new anti-pretexting rules, was implemented in 2007. That training is also required for new hires when they join the company or move to an affected group (e.g.,

² A reference to interconnected VoIP was added to Verizon Business' opt-in consent terms after the FCC's order applying CPNI rules to such services became effective.

sales, service or marketing). Additional function-specific training, as well as more informal question-and-answer sessions, were also provided on the new anti-pretexting requirements. Online CPNI resources provide standard forms as well as methods and procedures on how to properly handle CPNI in various situations.

Pursuant to section 64.2009(c), Verizon Business maintains records of all marketing and sales campaigns that use its customers' CPNI, and all instances in which CPNI is disclosed or access provided to third parties. Campaign records include a description of the campaign, the CPNI that was used in the campaign, and what products or services were offered as part of the campaign. Records are retained for at least one year.

Verizon Business has established a supervisory review process to ensure that its outbound marketing complies with the CPNI rules. Sales personnel must obtain supervisory approval for any proposed outbound marketing request for customer approval. Moreover, requests for CPNI approval must be reviewed and approved by the Verizon Business legal department. More generally, all Verizon Business outbound marketing is supervised by sales, service and/or marketing department management, as applicable, with the advice of the Verizon Business legal department. The sales, service and marketing departments also have designated CPNI compliance managers to oversee their respective departments' compliance activities. A dedicated CPNI questions email mailbox also has been established to make it easier for employees to obtain guidance on CPNI questions.

This statement of compliance is preceded by a certificate signed by an officer of Verizon Business, pursuant to section 64.2009(e). An explanation of actions taken against data brokers and summary of customer complaints concerning the unauthorized release of CPNI is attached below.

As noted above, Verizon Business does not seek opt-out customer CPNI approvals, so the safeguards required for opt-out approvals under subsection 64.2009(f) do not apply.

Rule § 64.2010 Safeguards on the Disclosure of Customer Proprietary Network Information

Verizon Business has taken reasonable procedural and technological measures to discover and protect against unauthorized CPNI access. In particular, Verizon Business's operational procedures do not permit disclosure of CPNI on inbound calls, except as may be permitted to previously authenticated customers under an agreement to protect CPNI between Verizon Business and customers subject to the business customer exception set forth in subsection 64.2010(g). Verizon Business does not disclose CPNI based on an in-store visit because it does not operate retail stores. Verizon Business requires that representatives of its customers be properly authenticated and provide a password as required by this section before CPNI is disclosed online.

As noted above, Verizon Business requires a password for any online access to CPNI, which is not prompted by asking for readily-available biographical information or account information. Before being allowed a password for online access to CPNI, Verizon Business procedures require any end user to be authenticated by means other than account information or readily-available biographical information.

Verizon Business has established procedures to immediately notify the affected customer when a password, customer back-up authentication response, online account, or address of record is created or changed, except at service initiation. Such notices do not reveal the changed information and are generally sent to a customer address of record (as defined by subsection 64.2003(b)) but not to the new address of record.

Rule § 64.2011 Notification of Customer Proprietary Network Information Security Breaches

Verizon Business has implemented procedures to notify law enforcement, and subsequently customers, of CPNI breaches (defined in subsection 64.2011(e)), as required by this section. Internal procedures direct information about possible CPNI breaches to a centralized email address, which makes that information available to a team including Verizon security, privacy and legal groups. Such possible breaches are then investigated and handled according to the requirements of this section.

In particular, Verizon Business procedures require that the United States Secret Service (“USSS”) and the Federal Bureau of Investigation (“FBI”) be notified of a CPNI breach through the central reporting facility required under subsection 64.2011(b) as soon as practicable, and in no event more than seven business days after Verizon Business reasonably determines that the breach has occurred. Customers and the public will not be notified of a CPNI breach during the seven business days after notification has been given to the USSS and FBI, except as permitted under subsections 64.2011(b)(2) in case of extraordinarily urgent need, to avoid immediate and irreparable harm, and after consulting and cooperating with the relevant investigative agency to minimize any adverse effects of the customer notification. If the relevant investigating agency directs Verizon Business in writing not to disclose to or notify customers or the public of a CPNI breach because such disclosure or notice would impede or compromise an ongoing or potential criminal investigation or national security, as provided by subsection 64.2011(b)(3), Verizon Business will further delay notifying or disclosing the CPNI breach to customers and the public. After Verizon Business has completed the process of notifying law enforcement of a CPNI breach, including the required periods of delay noted above, Verizon Business procedures require that the affected customer be notified of the breach. Records of CPNI breaches, notifications to the USSS and FBI pursuant to subsection 64.2011(b), and notifications to customers, will be kept and maintained for at least two years. Those records will include, if available, the dates the CPNI breach was discovered, the dates notifications were made, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Information Concerning Data Brokers and Complaints of Unauthorized Disclosure

Explanation of Actions Against Data Brokers³:

Verizon Business did not take any actions against data brokers in 2007.

Information of Verizon about Processes Used by Pretexters to Access CPNI and Verizon Actions in Response to Protect CPNI⁴:

Verizon Business is not aware of any processes used by pretexters not already in the record of the FCC's CPNI docket. The actions Verizon Business is taking in response to protect CPNI from pretexters are described in the other parts of this compliance statement.

Summary of the Number of Customer Complaints in 2007 Concerning Unauthorized Release of CPNI:

Verizon's summary of substantiated customer complaints follows.⁵

Verizon Business has records of 5 sustained customer complaints in 2007 concerning the unauthorized release of CPNI. The complaints are categorized as follows (using categories in Commission orders). Some complaints fall in more than one category.

Instances of improper access by employees: 0;

Instances of improper disclosure to individuals not authorized to receive the information: 5; and

Instances of improper access to online information by individuals not authorized to view the information: 2.

³ Under Commission rules, "actions" are proceedings instituted or petitions filed by a carrier at either state commissions, the court system, or at the Commission against data brokers

⁴ Under Commission rules, carriers must report information that they have with respect to the processes pretexters are using to attempt to access CPNI, and the steps carriers are taking to protect CPNI.

⁵ Because the rule to report such complaints did not become effective until December 8, 2007, during most of 2007, Verizon's Business recordkeeping systems were not designed to track such complaints for this purpose. In particular, Verizon Business systems did not maintain records of pre-December 8 complaints concerning unauthorized release of CPNI which, upon investigation, were not substantiated. Nevertheless, Verizon Business has provided information about pre-December 8, 2007 complaints where information was available.