

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

Annual 64.2009(e) CPNI Certification

Date: February 25, 2013

Name of companies covered by this Certification:

Verizon Business Global LLC*
Verizon Hawaii International Inc.
Verizon Select Services Inc.
Verizon Select Services of Virginia Inc.

Name of signatory: Michelle C. Ifill

Title of signatory: Senior Vice President, General Counsel and Secretary or Vice President

I, Michelle C. Ifill, certify that I am an officer of each of the Verizon entities listed above and, acting as an agent of these companies, I have personal knowledge that they have established operating procedures, as described in the attached statement, that, to the best of my knowledge, information and belief, and except as noted in the attached statement, 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 these companies' current operating procedures, as updated since last year's certifications, are designed to ensure that they are in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

Also attached are (1) an explanation of actions, if any, taken against data brokers, and (2) a summary of customer complaints received in 2012 concerning the unauthorized release of CPNI.

Signed: 

*Verizon Business Global LLC files a consolidated 499 for itself and all other Verizon Business Global LLC licensees not specifically listed.

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

Annual 64.2009(e) CPNI Certification

Date: February 25, 2013

Name of companies covered by this Certification:

Verizon New England Inc.
Verizon New York Inc.
Verizon Washington, DC Inc.
Verizon Delaware LLC
Verizon Maryland LLC
Verizon New Jersey Inc.
Verizon Pennsylvania LLC
Verizon Virginia LLC
Verizon California Inc.
Verizon Florida LLC
Verizon North LLC
Verizon South Inc.
GTE Southwest Incorporated d/b/a Verizon Southwest
Verizon Enterprise Solutions LLC
Verizon Long Distance LLC
Verizon Avenue Corp. d/b/a Verizon Enhanced Communities

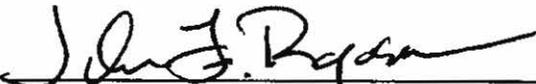
Name of signatory: John F. Raposa

Title of signatory: Vice President

I, John F. Raposa, certify that I am an officer of each of the Verizon entities listed above and, acting as an agent of these companies, I have personal knowledge that they have established operating procedures, as described in the attached statement, that, to the best of my knowledge, information and belief, and except as noted in the attached statement, 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 these companies' current operating procedures, as updated since last year's certifications, are designed to ensure that they are in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

Also attached are (1) an explanation of actions, if any, taken against data brokers, and (2) a summary of customer complaints received in 2012 concerning the unauthorized release of CPNI.

Signed: 

Verizon 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 “CPNI Rules”), Verizon¹ maintains a CPNI compliance program. The program is designed to communicate the CPNI rules and provide detailed information on how to comply with such rules. The Verizon legal organization manages the program and works with Verizon employees on a regular basis to review issues that may arise and to provide advice and guidance.

Section 64.2005 Use of Customer Proprietary Network Information Without Customer Approval

Verizon is a provider of local and long distance telecommunications and interconnected VoIP services to residential, business and government customers. CPNI is used, disclosed or accessed to provide or market Verizon service offerings to customers within the categories of services to which the customer already subscribes, to perform activities authorized under Section 222 of the Act and subsections 64.2005(b)(1), (c) and (d) of the CPNI Rules, and to comply with legal requirements (*e.g.*, lawful process). In addition, CPNI is shared among affiliated entities that provide service offerings to the customer. Verizon 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 obtains opt-out approval from its residential, small business and medium business voice customers to use CPNI to market communications-related services to its customers and to disclose CPNI to its agents and its affiliates for the purpose of marketing communications-related services.² With opt-out approval, Verizon also permits these agents and affiliates to access CPNI for such purposes.

Verizon obtains opt-in approval from its large business customers and a portion of its medium business and government customers to use CPNI to market products and services to its customers and to disclose CPNI to its agents, affiliates, contractors and partners for the purpose of marketing products and services. With opt-in approval, Verizon also permits these agents, affiliates, contractors and partners to access CPNI for such purposes.

Under both the opt-in and opt-out procedures, customer approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval. Verizon maintains records of customer approvals and disapprovals for at least one year.

¹ See list of Verizon entities on the Michelle C. Ifill and John F. Raposa Certifications.

² A subset of consumer, small business and medium business voice customers did not receive notice of Verizon’s request for opt-out approval on the initial bill. See Notification under Section 64.2009(f) – Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115 (Jan. 18, 2013) (“Verizon Notice”).

Verizon obtains one-time approval from its customers to use CPNI during customer service calls, chats, and online ordering and inquiry processes. Customer approval remains in effect only until the call, chat, or online ordering or inquiry process is complete. Verizon maintains records of customer notice for one-time use approvals for one year.

Section 64.2008 Notice Required for Use of Customer Proprietary Network Information

Verizon provides written opt-out notice to its residential, small business and medium business voice customers when they sign up for service and on a biennial basis thereafter.³ The notice defines CPNI and advises that CPNI may be used and shared with Verizon's affiliates and agents to offer a wide range of communications-related services that may be different from those they already buy from the Verizon family of companies. The notice explains 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 informs customers that the customer has a right, and Verizon has a duty to protect the confidentiality of CPNI. 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 Verizon to change it. Verizon adheres to a minimum 30-day waiting period when providing initial opt-out notices and allows at least three additional days for mailing before using CPNI under opt-out.

Verizon provides written opt-in notice to its large business and a portion of its medium business and government customers when soliciting opt-in approval to use, disclose or permit access to the customers' CPNI. The notice informs the customers of their rights to deny such approval, and provides sufficient information to enable the customers to make informed decisions as to whether to grant or deny the approval requested. The notice includes the following minimum 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 CPNI. The notice states that CPNI includes information relating to the quantity, technical configuration, type, destination, location, and amount of use of the telecommunications and interconnected VoIP services the customer purchases from Verizon, as well as related local and toll billing information, made available to Verizon solely by virtue of the customer relationship with Verizon. The notice seeks consent to share customer CPNI and other confidential information among the Verizon affiliates, and with agents and partners, so that all may use it to offer the customer a full range of products and services. The notice states that the customer's decision to consent or refuse consent will remain valid until the customer otherwise advises Verizon, and in either case, will not affect the provision of service to the customer. Opt-in notices state that the 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. The opt-in notice may be provided to the customer as a separate document, or in the customer's service agreement.

³ See Verizon Notice.

Verizon uses a notice to obtain customer approval for limited, one-time use of CPNI for the duration of a customer session. The notice complies with the requirements of this section.

Section 64.2009 Safeguards Required for Use of Customer Proprietary Network Information

Verizon has implemented systems designed to provide the status of a customer's CPNI approval prior to the use or disclosure of CPNI. When a customer's opt-in or opt-out CPNI election is received, it is recorded in Verizon systems, including the date of receipt. If the customer withdraws approval (including by a subsequent opt-out), the systems are updated to reflect such withdrawal (this does not apply to limited one-time approvals, which expire automatically at the end of the session). Sales, service and marketing personnel can reference the systems whenever needed to determine a customer's current CPNI approval status.

Verizon trains appropriate personnel about the CPNI rules and advises that the failure to follow them can be grounds for disciplinary action, up to and including dismissal. Such training is required for new hires and internal transfers when they first are assigned to an affected group (e.g., sales, service or marketing). Online CPNI resources provide standard forms as well as methods and procedures on how to properly handle CPNI in certain situations.

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

Verizon has a supervisory review process for outbound marketing designed to comply with the CPNI rules. Sales personnel must obtain supervisory approval of any proposed outbound marketing request for customer approval. Generally, all Verizon outbound marketing is supervised by sales, service and/or marketing department management, as applicable, with the advice of the Verizon legal department. The sales, service and marketing departments also have designated CPNI compliance managers to oversee their respective departments' compliance activities. A dedicated email mailbox is available for employees to obtain guidance on CPNI questions.

Verizon provides written notice to the Commission, within five business days after determination, should a failure of its 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, pursuant to section 64.2009(e). An explanation of actions taken against data brokers and a 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

Verizon uses reasonable procedural and technological measures designed to discover and protect against unauthorized CPNI access and comply with this section and applicable law. Verizon reviews and updates these measures periodically. Verizon's operational procedures require that customers or their representatives be properly authenticated, as required by this section, applicable law, and/or pursuant to contractual terms under the business customer exemption (BCE) in section 64.2010(g),⁴ before they are given access to CPNI. Verizon processes and procedures do not allow disclosure of call detail CPNI on inbound calls, except as permitted by law or under the BCE. Verizon will 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. Except as permitted by law or under the BCE, Verizon's online procedures do not grant online access to CPNI based on the presentation of readily available biographical or account information 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, Verizon's back-up authentication procedures do not rely on prompts to the customer for readily available biographical or account information. If a customer cannot provide a password or satisfy the back-up authentication process, the customer is denied online access and must be re-authenticated. Verizon'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.

Verizon reinforces its procedures through periodic observations, which include providing feedback to representatives when safeguarding processes are not properly followed. Employees also are trained annually on processes regarding proper safeguarding of customer accounts.

Verizon investigates and resolves any reports of potential unauthorized access to or disclosure of CPNI and takes appropriate corrective action as needed to maintain the effectiveness of its procedures and operations.

Verizon has established systems and procedures designed 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(q)). These notices are not triggered for customers under the BCE. In July 2012, Verizon entered into a Consent Decree, which provides for additional measures to promote compliance with section 64.2010(f). Verizon has implemented those measures.

⁴ Verizon occasionally binds itself contractually to authentication regimes other than those described in Section 64.2010 of the Federal Communications Commission's rules for services provided to certain business customers that have both a dedicated account representative and a contract that specifically addresses its protection of CPNI.

Section 64.2011 Notification of customer proprietary network information security breaches

Verizon 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 Verizon 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.

Verizon 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 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 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 will further delay notifying or disclosing the CPNI breach to customers and the public. After Verizon has completed the process of notifying law enforcement of a CPNI breach, including the required periods of delay noted above, Verizon 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 that 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:⁵

Verizon did not take any actions against data brokers in 2012.

Information of Verizon about Processes Used by Pretexters to Access CPNI and Verizon Actions in Response to Protect CPNI:⁶

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

Summary of the Number of Customer Complaints in 2012 Concerning Unauthorized Release of CPNI

Verizon's summary of 2012 CPNI complaints by category appears below. A review of allegations revealed 8 substantiated complaints by customers involving unauthorized access to the customer's CPNI, or unauthorized disclosure of the customer's CPNI:

Number of complaints involving improper access by employees: 0

Number of complaints involving improper disclosure to unauthorized individuals: 1

Number of complaints involving improper online access by unauthorized individuals: 7

⁵ 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.

⁶ 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.