



Tamara Preiss
Vice President
Federal Regulatory and Legal Affairs
1300 I Street, NW, Suite 500 East
Washington, DC 20005
Phone 202.515.2540
Fax 202.336.7922
tamara.preiss@verizon.com

February 27, 2019

VIA ECFS

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

Re: Annual CPNI Certification, EB Docket No. 06-36

Dear Ms. Dortch:

Pursuant to Section 64.2009(e) of the Commission's rules, 47 C.F.R. § 64.2009(e), Verizon, on behalf of the identified operating entities, hereby files its annual certifications of compliance with the Commission's customer proprietary network information (CPNI) rules.

Please contact the undersigned should you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Jonathan Preiss". The signature is written in a cursive, flowing style.

Attachments

cc: Best Copy and Printing, Inc. (via e-mail)

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

Annual 64.2009(e) CPNI Certification

Date: February 25, 2019

Name of companies covered by this Certification (collectively "Verizon"): See attached.

Name of signatory: Steven Tugentman

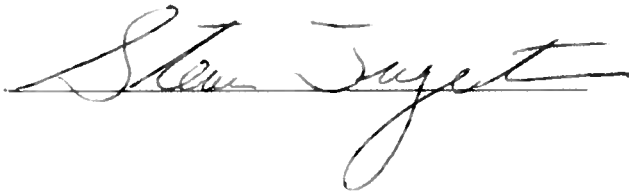
Title of signatory: Senior Vice President, Vice President, General Counsel, Secretary

I, Steven Tugentman, certify that I am an officer of each of the Verizon entities listed in the attached 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 the last certification, 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 2018 concerning the unauthorized release of CPNI.

Signed: _____

A handwritten signature in black ink, appearing to read "Steven Tugentman", written over a horizontal line.

Legal Entities Covered by the Verizon CPNI Certification

Cellco Partnership¹
Badlands Cellular of North Dakota Limited Partnership²
Colorado 7 Saguache Limited Partnership¹
San Isabel Cellular of Colorado Limited Partnership⁴
MCI Communications Corporation⁵
Ventures XXV Inc.⁶
Verizon Delaware LLC
Verizon Hawaii International Inc.
Verizon Long Distance LLC
Verizon Maryland LLC
Verizon New England Inc.
Verizon New Jersey Inc.
Verizon New York Inc.
Verizon North LLC
Verizon Pennsylvania LLC
Verizon Select Services Inc.
Verizon Select Services of Virginia Inc.
Verizon South Inc.
Verizon Virginia LLC
Verizon Washington, DC Inc.
XO Communications Services, LLC⁷

¹ Cellco Partnership files a consolidated 499 for itself and all other Cellco Partnership licensees not listed.

² Steve Tugentman is an officer of CommNet Cellular Inc., this Limited Partnership's Managing Agent.

³ Steve Tugentman is an officer of CommNet Cellular Inc., this Limited Partnership's Manager.

⁴ Steve Tugentman is an officer of CommNet Cellular Inc., this Limited Partnership's Manager.

⁵ MCI Communications Corporation files a consolidated 499 for itself and all other MCI Communications Corporation licensees not listed.

⁶ Verizon Avenue Corp. d/b/a Verizon Enhanced Communities is now Ventures XXV Inc.

⁷ XO Communications Services, LLC files a consolidated 499 for itself and all other XO Communications Services, LLC licensees not listed.

Verizon^{*}
CPNI Statement of Compliance

**Section 64.2005 Use of Customer Proprietary Network Information Without
Customer Approval**

Verizon is a provider of mobile wireless and wireline telecommunications and interconnected VoIP services to consumer, business, and government customers. CPNI is used, disclosed, or accessed to provide or market Verizon services to customers within the categories of services to which the customer already subscribes (known as the "total service approach" authorized by section 64.2005(a) of the CPNI Rules), to perform activities authorized under Section 222 of the Communications Act of 1934, as amended (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 operating procedures do not permit use of, disclosure of, or 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 has procedures to seek opt-out approval from its consumer and some of its business customers to use CPNI to market communications-related services and to disclose CPNI to its agents and its affiliates for the purpose of marketing communications-related services. With opt-out approval, Verizon also permits these agents and affiliates to access CPNI for such purposes.

Verizon has procedures to seek opt-in approval from some of its consumer and business customers for the purpose of using and sharing CPNI with affiliates to provide relevant marketing messages from Verizon and other companies. Verizon also has procedures to seek opt-in approval from some of its consumer and business customers to use and share CPNI with third parties for their purposes. Verizon also has procedures to seek opt-in approval from some of its business customers and a portion of its government customers to use CPNI to market products and services and to disclose CPNI to its agents, affiliates, contractors and partners for the purpose of marketing products and services. With this 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.

In certain circumstances, Verizon has procedures to seek 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.

^{*} See list of Verizon entities attached to the Certification signed by Steven Tugentman.

Section 64.2008 Notice Required for Use of Customer Proprietary Network Information

Verizon operating procedures require the placement of an opt-out notice on the invoice (whether electronic or paper) to Verizon consumer and business customers for whom Verizon relies on opt-out consent. The contents of the notice provided to these customers comply with the general requirements for notices and the specific requirements for opt-out notices set forth in section 64.2008, although the specific language used to convey it may vary. The notice provides sufficient information to enable the customers to make informed decisions as to whether to grant or deny the approval requested. 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 informs customers that the customer has a right and Verizon has a duty to protect the confidentiality of CPNI. 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 advises customers that they can opt out by dialing the toll free number provided in the notice. Some customers are also provided an option to opt out through the Verizon on-line platform or by calling customer care during regular business hours. The toll free service and on-line platform are 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 operating procedures require a minimum 30-day waiting period when providing initial opt-out notices and allows for at least three additional days when mailing the initial opt-out notices before using CPNI under opt-out.

Verizon operating procedures require that an opt-in notice be provided to Verizon consumer, business, and government customers when soliciting opt-in approval to use, disclose or permit access to the customers' CPNI to market products and services or for other purposes. The contents of the notices provided to these customers comply with the general requirements for notices and the specific requirements for opt-in notices set forth in section 64.2008 and include the following minimum content, although the specific language used to convey it may vary. The notices define CPNI and advise, to the extent applicable, that CPNI may be used and shared with Verizon's affiliates, agents, contractors and partners for the purpose of marketing products and services or other purposes. The notices inform customers that the customer has a right and Verizon has a duty to protect the confidentiality of CPNI. The notices inform the customers of their right to deny approval and provide sufficient information to enable the customers to make informed decisions as to whether to grant or deny the approval requested. The notices state that the customer's decision to consent or refuse consent will remain valid until the customer otherwise advises Verizon. The notices communicate that the denial or withdrawal of consent will not affect provisioning of services to which the customer subscribes and that the customer may withdraw consent at any time.

The opt-out and opt-in notices are typewritten in sufficiently large font, and are provided in a manner so as to be readily apparent to the customer. If any portion of the notices is translated into another language, then all portions of the notices are translated into that language.

Verizon operating procedures require that notice be provided to obtain customer approval for limited, one-time use of CPNI for the duration of a customer session. The notices are provided through oral, electronic, or written methods and comply with the requirements for opt-in and one-time use notices set forth in section 64.2008.

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, Verizon procedures require that the election be recorded in Verizon systems. If the customer withdraws approval (including by a subsequent opt-out), Verizon has procedures to update the systems to reflect such withdrawal (this does not apply to limited one-time approvals, which expire automatically at the end of the session).

Verizon trains appropriate employees 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 provides instruction on Verizon's practices and procedures for CPNI compliance as well as contact information for CPNI inquiries and concerns. The training states that employees may be subject to discipline for failure to comply with Verizon's CPNI operating procedures. The disciplinary process may include coaching, written reports, or other actions, including termination. In addition to providing contacts for CPNI inquiries and concerns, online CPNI resources provide standard forms as well as methods and procedures on how to properly handle CPNI in certain situations.

Verizon has procedures to maintain records of 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. Verizon procedures require that records be retained for at least one year.

Verizon has a supervisory review process for outbound marketing designed to comply with the CPNI rules. Verizon procedures require that personnel obtain supervisory approval of any proposed outbound marketing request for customer approval.

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'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 in section 64.2010(g),⁹ 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 business customer exemption. Verizon procedures require online access to CPNI be provided in accordance with the heightened authentication requirements of section 64.2010(e) or pursuant to the business customer exemption in accordance with section 64.2010(g). 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, Verizon procedures require that the customer be denied online access, and the customer must be re-authenticated. Verizon procedures require that representatives disclose CPNI at retail locations only to customers who present valid government-issued photo IDs.

Verizon maintains procedures to notify customers through an e-mail, letter, text, or voice message whenever a password, customer response to a back-up means of authentication, online account, or address of record is created or changed, except when service is initiated. 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 may not be triggered for customers under the business customer exemption.

Section 64.2011 Notification of customer proprietary network information security breaches

In the event a breach reportable under section 64.2011 occurs, Verizon has established the following notification procedures: No later than seven business days after determination of a CPNI breach, as defined in section 64.2011(e), Verizon notifies law enforcement through the reporting facility maintained at <https://www.cpnireporting.gov/cpni/content/disclaimer.seam>. Verizon does not notify its customers of or publicly disclose the breach until at least seven full business days have passed after notification of law enforcement, unless Verizon believes there is an extraordinarily urgent need to notify any class of affected customers before that time. If the relevant investigating agency directs Verizon not to disclose the breach beyond the seven-business day period, in accordance with section 64.2011(b)(3), Verizon will not disclose the breach until the agency provides notice that disclosure will no longer impede or compromise a criminal investigation or national security. After completing the process of notifying law enforcement in accordance with section 64.2011(b), Verizon procedures require notification to

⁹ 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.

its customers of the breach of those customers' CPNI. Verizon maintains records of breaches, notification to law enforcement, and customer notification for at least two years. Those records include, when available, dates of discovery and notification, descriptions of the CPNI that was breached, and the circumstances of the breach.

Information Concerning Data Brokers and Complaints of Unauthorized Disclosure

Explanation of Actions against Data Brokers:¹⁰

Verizon did not take any actions against data brokers in 2018.

Information of Verizon about Processes Used by Pretexters to Access CPNI and Verizon Actions in Response to Protect CPNI:¹¹

Many of the processes pretexters are using are materially the same as those described in the record of the FCC's CPNI docket. In addition, Verizon notes the following trends: (i) pretexters are using information from a number of different sources, including confidential information obtained from other organizations or companies as well as public sources; (ii) pretexters are using mechanized processes; (iii) pretexters continue to use processes to obtain CPNI for purely personal reasons (for example, to determine whom an ex-spouse is calling), and (iv) pretexters also attempt to compromise accounts for other purposes. For example, pretexters may attempt to compromise a customer's Verizon account for financial gain, including equipment fraud; or to compromise a customer's non-Verizon accounts, including social media, bank and cryptocurrency accounts. 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 2018 Concerning Unauthorized Release of CPNI:

Verizon's summary of 2018 CPNI complaints by category appears below. A review of allegations revealed 36 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: 6

Number of complaints involving improper disclosure to unauthorized individuals: 8

Number of complaints involving improper online access by unauthorized individuals: 22

¹⁰ 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.

¹¹ 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.

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

Annual 64.2009(e) CPNI Certification

Date: February 25, 2019

Name of companies covered by this Certification: Verizon Connect Inc.

Name of signatory: Alexis Toro

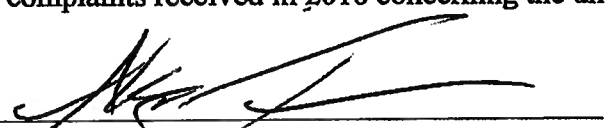
Title of signatory: Vice President and Chief Financial Officer

I, Alexis Toro, certify that I am an officer of Verizon Connect and, acting as an agent of this company, I have personal knowledge that it has 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 this company's current operating procedures, as updated since our last certification, are designed to ensure that it is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

Also attached is an explanation of actions, if any, taken against data brokers, and a summary of customer complaints received in 2018 concerning the unauthorized release of CPNI.

Signed: _____



Verizon Connect Inc. (Connect)
CPNI Statement of Compliance

**Section 64.2005 Use of Customer Proprietary Network Information Without
Customer Approval**

Connect provides telecommunications services to one customer. Connect has not used and does not plan to use CPNI for marketing that requires consent.

**Section 64.2007-8 Approval Required for Use of Customer Proprietary Network
Information; Notice Required for Use of Customer Proprietary
Network Information**

Connect does not use, disclose, or permit access to CPNI to market services that are not within a category of services to which the customer already subscribes. Thus, Connect does not send notification or request corresponding approval from its customer. Connect does not use or share CPNI with joint venture partners or independent contractors to market to its customer.

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

Connect 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.

This statement of compliance is preceded by a certificate signed by an officer of Connect, 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 below.

Although Connect currently does not use, disclose, or permit access to CPNI to market services, if it chooses to change this policy and use CPNI for marketing, it will (1) implement a system by which the status of a customer's CPNI approval can be clearly established, (2) maintain a record of its and its affiliates' sales and marketing campaigns that use its customers' CPNI for at least one year, (3) maintain a record of all instances where CPNI was disclosed or provided to third parties for at least one year, (4) require sales personnel to obtain supervisory approval of any proposed outbound marketing request for customer approval, and (5) provide written notice to the FCC within five business days of any instance where its opt-out mechanism did not work properly.

Section 64.2010 Safeguards on the disclosure of customer proprietary network information

Connect has an assigned representative to work with the single customer receiving telecommunications service. The dedicated Connect representative discloses CPNI to the customer through a representative authorized by the customer contractually. Connect does not provide in-store access or online access to CPNI. Whenever a significant account change occurs, Connect immediately notifies the customer of the change at an address of record.

Section 64.2011 Notification of customer proprietary network information security breaches

Connect has implemented procedures to notify law enforcement, and subsequently customers, of CPNI breaches (defined in subsection 64.2011(e)). Internal procedures direct employees to notify the legal department of any potential CPNI breach. When a breach is confirmed, the appropriate personnel are prepared to make the required notifications to the United States Secret Service, the Federal Bureau of Investigation, and the customer. Records of such breaches and the corresponding notifications are maintained for at least two year.

Information Concerning Data Brokers and Complaints of Unauthorized Disclosure

Explanation of Actions Against Data Brokers:

Connect did not take any actions against data brokers in 2018.

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

Connect is not aware of any processes used by pretexters materially different from what is in the record of the Federal Communications Commission's CPNI docket. The actions Connect 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 2018 Concerning Unauthorized Release of CPNI

Connect's summary of 2018 CPNI complaints by category appears below.

Number of complaints involving improper access by employees: 0

Number of complaints involving improper disclosure to unauthorized individuals: 0

Number of complaints involving improper online access by unauthorized individuals: 0

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

Annual 64.2009(e) CPNI Certification

Date: February 27, 2019

Name of companies covered by this Certification: Visible Service LLC ("Visible")

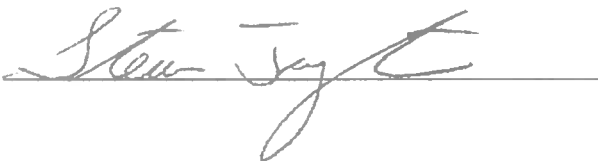
Name of signatory: Steven Tugentman

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

I, Steven Tugentman, certify that I am an officer of Visible and, acting as an agent of Visible, 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 Visible's current operating procedures 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 is an explanation of actions, if any, taken against data brokers, and a summary of customer complaints received in 2018 concerning the unauthorized release of CPNI.

Signed: 

Visible
CPNI Statement of Compliance

Section 64.2005 Use of Customer Proprietary Network Information Without Customer Approval

CPNI is used, disclosed, or accessed to provide or market Visible services to customers within the categories of services to which the customer already subscribes (known as the "total service approach" authorized by section 64.2005(a) of the CPNI Rules), to perform activities authorized under Section 222 of the Communications Act of 1934, as amended (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. Visible operating procedures do not permit use, disclosure of, or 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

Visible has procedures to seek opt-out approval from its customers to use CPNI to market communications-related services and to disclose CPNI to its agents and its affiliates for the purpose of marketing communications-related services. With opt-out approval, Visible also permits these agents and affiliates to access CPNI for such purposes. A customer's approval or disapproval remains in effect until the customer revokes or limits such approval or disapproval.

Section 64.2008 Notice Required for Use of Customer Proprietary Network Information

Visible operating procedures require the placement of an opt-out notice on the electronic invoice provided to Visible customers for whom Visible relies on opt-out consent. The contents of the notice provided to these customers comply with the general requirements for notices and the specific requirements for opt-out notices set forth in section 64.2008, although the specific language used to convey it may vary. The notice provides sufficient information to enable the customers to make informed decisions as to whether to grant or deny the approval requested. The notice defines CPNI and advises that CPNI may be used and shared with Visible's affiliates and agents to offer a wide range of communications-related services that may be different from those they already buy from Visible. The notice informs customers that the customer has a right, and Visible has a duty to protect the confidentiality of CPNI. 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 advises customers that they can opt out through the Visible on-line platform. The on-line platform 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 Visible to change it. Visible operating procedures require a minimum 30-day waiting period when providing initial opt-out notices.

The opt-out notice is typewritten in sufficiently large font and provided in a manner so as to be readily apparent to the customer. If any portion of the notices is translated into another language, then all portions of the notices are translated into that language.

Section 64.2009 Safeguards Required for Use of Customer Proprietary Network Information

Visible 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-out CPNI election is received, Visible procedures require that the election be recorded in Visible systems. If the customer withdraws approval (including by a subsequent opt-out), Visible has procedures to update the systems to reflect such withdrawal.

Visible trains appropriate employees 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 provides instruction on practices and procedures for CPNI compliance as well as contact information for CPNI inquiries and concerns. The training states that employees may be subject to discipline for failure to comply with CPNI operating procedures. The disciplinary process may include coaching, written reports or other actions, including termination.

Visible has procedures to maintain records of 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. Visible procedures require that records be retained for at least one year.

Visible has a supervisory review process for outbound marketing designed to comply with the CPNI rules. Visible procedures require that personnel obtain supervisory approval of any proposed outbound marketing request for customer approval.

Visible 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 Visible, 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

Visible's operational procedures require that customers or their representatives be properly authenticated, as required by this section before they are given access to CPNI. Visible processes and procedures do not allow disclosure of call detail CPNI on inbound calls, except as permitted by law. Visible procedures require online access to CPNI be provided in accordance with the heightened authentication requirements of section 64.2010(e). In the event of a lost or forgotten password, Visible'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, Visible procedures require that the customer be denied online access, and the customer must be re-authenticated.

Visible maintains procedures to notify customers through an e-mail or text message whenever a password, customer response to a back-up means of authentication, online account, or address of record is created or changed, except when service is initiated. 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)).

Section 64.2011 Notification of customer proprietary network information security breaches

In the event a breach reportable under section 64.2011 occurs, Visible has established the following notification procedures: No later than seven business days after determination of a CPNI breach, as defined in section 64.2011(e), Visible notifies law enforcement through the reporting facility maintained at <https://www.cpnireporting.gov/cpni/content/disclaimer.seam>. Visible does not notify its customers of or publicly disclose the breach until at least seven full business days have passed after notification of law enforcement, unless Visible believes there is an extraordinarily urgent need to notify any class of affected customers before that time. If the relevant investigating agency directs Visible not to disclose the breach beyond the seven-business day period, in accordance with section 64.2011(b)(3), Visible will not disclose the breach until the agency provides notice that disclosure will no longer impede or compromise a criminal investigation or national security. After completing the process of notifying law enforcement in accordance with section 64.2011(b), Visible procedures require notification to its customers of the breach of those customers' CPNI. Visible maintains records of breaches, notification to law enforcement, and customer notification for at least two years. Those records include, when available, dates of discovery and notification, descriptions of the CPNI that was breached, and the circumstances of the breach.

Information Concerning Data Brokers and Complaints of Unauthorized Disclosure

Explanation of Actions against Data Brokers:

Visible did not take any actions against data brokers in 2018.

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

Many of the processes pretexters are using are materially the same as those described in the record of the FCC's CPNI docket. The actions Visible 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 2018 Concerning Unauthorized Release of CPNI:

Visible's summary of 2018 CPNI complaints by category appears below.

Number of complaints involving improper access by employees: 0

Number of complaints involving improper disclosure to unauthorized individuals: 0

Number of complaints involving improper online access by unauthorized individuals: 0