

BEFORE
THE FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

EB-06-TC-060

EB Docket No. 06-36

ANNUAL 47 C.F.R. § 64.2009(e) CPNI CERTIFICATION

Annual 64.2009(e) CPNI Certification for 2017

Date filed: **February 27, 2018**

Name of company covered by this certification: Doylestown Telephone Company

Form 499 Filer ID: **809678**

Name of signatory: **Thomas J. Brockman**

Title of signatory: President

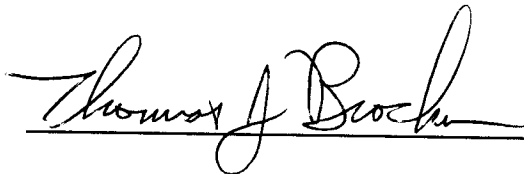
I, Thomas J. Brockman, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system or at the Commission) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



DOYLESTOWN TELEPHONE COMPANY

STATEMENT OF CPNI PROCEDURES

Doylestown Telephone Company has created a CPNI Policy Handbook containing the following procedures that it has adopted to ensure the protection of CPNI. The handbook describes our procedures in greater detail and provides practical guidance on how to protect against unauthorized disclosure or use of CPNI. The handbook is distributed to our employees during training and serves as an important reference tool for our employees.

Duty to Protect CPNI

We as a communications company recognize our duty to protect customer CPNI. We may not disclose CPNI to unauthorized persons, nor may we use CPNI in certain ways without consent from our customers. Before we can provide customers with their own CPNI, we must authenticate the customer.

We recognize that there are a few cases in which we can disclose CPNI without first obtaining customer approval:

1. Administrative use: We may use CPNI to *initiate, render, bill and collect* for communications services.
2. Protection of carrier and third parties: We may use CPNI to protect the interests of our company, such as to prevent fraud or illegal use of our systems and network. Employees are notified of the steps to take, if any, in these sorts of situations.
3. As required by law: We may disclose CPNI if we are required to by law, such as through legal process (subpoenas) or in response to requests by law enforcement. Employees are notified of any steps they must take in these situations.

Our Own Use Of CPNI

We may use CPNI to provide or market services to our existing customers. We understand that we are required to obtain customer approval prior to using CPNI in certain ways.

Marketing

We understand that we do not need to obtain customer approval before using CPNI to market services to our existing customers within the categories of service to which the customer already subscribes.

We understand that we may not use CPNI to market services that are in a service category to which the customer does not already subscribe without customer approval.

We understand that we cannot use CPNI to solicit a customer to add a new category of service without first obtaining the customer's approval.

We also understand that we do not need customer consent before using CPNI to market "adjunct-to-basic" services such as speed dialing, computer-provided directory assistance, call monitoring, call

tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain centrex features.

We understand that we may not use CPNI to identify or track customers that call competing service providers.

We regularly review our marketing practices to determine when and how CPNI is used within the company, and whether CPNI is being shared with other entities. We also review new marketing or sales campaigns to ensure compliance with these CPNI policies and with the FCC's CPNI regulations. We do not share CPNI with any affiliates or other third parties.

Provision of Services

We understand that we do not need customer approval to use CPNI to provide CPE and call answering, voice mail or messaging, voice storage and retrieval services, fax store and forward, and protocol conversion.

Authenticating Customers Before Disclosing CPNI

We understand that we are required to objectively determine that our customers are who they say they are before disclosing CPNI to them.

Telephone

We understand that when a customer calls, we may not release *call detail information*, or information relating to the transmission of specific telephone calls until we have obtained the account password from the caller, or called the customer back at the telephone number of record to ensure that the customer is who s/he says s/he is. Alternatively, we may offer to send the call detail information to the address of record or provide it to the customer or an authorized individual in person after s/he has produced valid photo identification at our office.

We understand that we may disclose *non-call detail information* over the telephone after authenticating the customer by calling back the telephone number of record, checking valid photo identification, or by mailing the information to the account address of record.

In-Person Authentication

We understand that before we can disclose CPNI to customers in person, the customer must present *valid government-issued photo identification*. The name on the photo identification must match the name on the account. If the customer cannot present the required identification, we offer to provide the requested CPNI by sending it to the account address of record.

Mail

If the customer requests CPNI through regular mail, or if the customer cannot comply with one of the authentication methods above, we send the requested information to the customer's address of record only.

Online Access

We password protect online access to CPNI. New customers establish passwords at service initiation. Our existing customers obtain their passwords by U.S mail to the billing address on record. We do not allow customers to choose passwords based on their readily available biographical information or account data. Customer passwords will be further subject to the following restrictions: They must be at least four (4) characters long.

After a customer has made 3 failed attempts to log into his/her online account, we block online access to the account for security purposes. Customers locked out of their online accounts must contact our office to regain online account access.

If a customer loses or forgets his/her online account password, the customer may answer a series of security questions in order to gain access to the account. The customer is then given the opportunity to choose a new password. Again, if the customer fails to provide the correct answer to the security questions, we block online access to the account for security purposes. These customers must contact our office to regain online access.

Customer Notification of CPNI Rights

We provide a CPNI privacy policy to all customers annually, as a bill insert in the December bill. This policy provides notification to each customer of his/her right to restrict use of, disclosure of, and access to that customer's CPNI. We maintain a list of all customers who receive the privacy policy, the date on which the policy is sent, and a copy of the policy in our records for one (1) year following the mailing of the policy. We provide additional copies of the CPNI privacy policy to all customers who request it and to all new customers upon activation of service.

The policy contains an opt-out customer approval notice. Customers who do not wish to allow us to use their CPNI to market services outside their existing service categories, or who do not wish to allow us to share their CPNI with affiliates, have 30 days to contact us to tell us that they do not approve of this use. If we do not hear back from the customer within 30 days, we understand that we are free to use their CPNI for these purposes. We understand that customers can change their option at any time by contacting us, and we notify our customers of this right.

We maintain records of the customers who received the opt-out approval notice and records of the customers who contacted us to opt out in accordance with our record-keeping policies.

We understand that we must provide written notice to the FCC within five (5) business days if our opt-out mechanisms do not work properly to the degree that our customers' inability to opt out is more than an anomaly.

Training And Discipline

We trained all of our employees regarding the company's CPNI policies prior to the effective date of the most recent CPNI regulations, December 8, 2007. Employees are required to attend an annual retraining to ensure that they understand the company's CPNI policies and any updates to those policies. New employees who will have access to CPNI are trained when they join the company, and then attend the regularly-scheduled retraining sessions. At the conclusion of each training session, employees are asked to sign certificates stating that they understand the company's CPNI policies and that they will comply with those policies.

We have implemented the following disciplinary guidelines for employees who fail to follow our CPNI policies:

Disciplinary Actions

This Disciplinary Actions Policy applies to all regular employees who have completed the Introductory Period.

This policy pertains to matters of conduct as well as the employee's competence. However, an employee who does not display satisfactory performance and accomplishment on the job may be dismissed, without resorting to the steps set forth in this policy.

Under normal circumstances, managers are expected to follow the procedure outlined below. There may be particular situations, however, in which the seriousness of the offense justifies the omission of one or more of the steps in the procedure. Likewise, there may be times when the company may decide to repeat a disciplinary step.

Discipline Procedure

Unacceptable behavior which does not lead to immediate dismissal may be dealt with in the following manner:

1. Oral Reminder
2. Written Warning
3. Decision-Making Paid Leave
4. Termination

To ensure that Doylestown Telephone Company business is conducted properly and efficiently, you must conform to certain standards of attendance, conduct, work performance and other work rules and regulations. When a problem in these areas does arise, your manager will coach and counsel you in mutually developing an effective solution. If, however, you fail to respond to coaching or counseling, or an incident occurs requiring formal discipline, the following procedures occur.

Step One: Oral Reminder

Your manager will meet with you to discuss the problem or violation, making sure that you understand the nature of the problem or violation and the expected remedy. The purpose of this conversation is to remind you of exactly what the rule or performance expectation is and also to remind you that it is your responsibility to meet Doylestown Telephone Company's expectations.

You will be informed that the Oral Reminder is the first step of the discipline procedure. Your manager will fully document the Oral Reminder, which will remain in effect for three (3) months. Documentation of the incident will remain in the confidential department file and will not be placed in your personnel record, unless another disciplinary event occurs.

Step Two: Written Warning

If your performance does not improve within the three (3) month period, or if you are again in violation of Doylestown Telephone Company practices, rules or standards of conduct, your manager will discuss the problem with you, emphasizing the seriousness of the issue and the need for you to immediately remedy the problem. Your manager will advise you that you are now at the second formal level of disciplinary action. After the meeting your manager will write a memo to you summarizing the discussion and your agreement to change. A copy of the memo to be sent to your personnel file.

The Written Warning will remain in effect for three (3) months.

Step Three: Decision-Making Leave / Counseling Session

If your performance does not improve within the three (3) month period following the Written Warning, or if you are again in violation of Doylestown Telephone Company practices, rules or standards of conduct, you will be placed on Decision-Making Leave. The Decision-Making Leave is the third and final step of Doylestown Telephone Company's disciplinary process.

Decision-Making Leave is a paid, one- (1) day disciplinary suspension. Employees on Decision-Making Leave will spend the following day away from work deciding whether to commit to correcting the immediate problem and to conform to all of the company's practices, rules and standards of conduct, or to quit and terminate their employment with Doylestown Telephone Company.

If your decision following the Decision-Making Leave is to return to work and abide by Doylestown Telephone Company practices, rules and standards of conduct, your manager will write a letter to you explaining your commitment and the consequences of failing to meet this commitment. You will be required to sign the letter to acknowledge receipt. A copy will be placed in your personnel file.

You will be allowed to return to work with the understanding that if a positive change in behavior does not occur, or if another disciplinary problem occurs within the next three (3) months, you will be terminated.

If you are unwilling to make such a commitment, you may either resign or be terminated. Disciplinary records are maintained in the company files in accordance with our record-keeping policies.

Record-Keeping

We maintain the following records in our files for one (1) year:

- a. Records relating to the annual mailing of the customer CPNI privacy policy;
- b. Records of customer approval or disapproval of CPNI use, or the limitation or revocation thereof;
- c. Records of disclosure or provision of CPNI to third parties for marketing purposes, including Doylestown Telephone Company's and affiliates' sales and marketing campaigns using customer CPNI, the CPNI used, and what products and services were offered as part of the campaign; and
- d. Employee disciplinary records.

We maintain records of discovered CPNI breaches, notifications to law enforcement regarding breaches, and any responses from law enforcement regarding those breaches, in our files for at least two (2) years.

Notification Of Account Changes

We understand that we are required to notify customers when changes have been made to passwords, customer responses to back-up means of authentication, online accounts, or addresses of record by mailing a notification to the account address of record.

We do not reveal the changed account data in the notification.

Unauthorized Disclosure Of CPNI

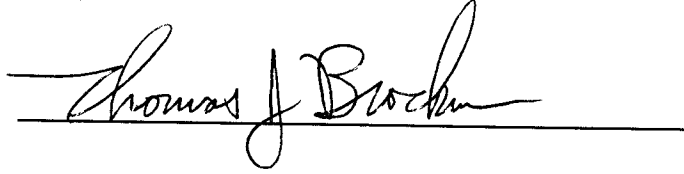
We understand that we must report CPNI breaches to law enforcement no later than seven (7) business days after determining the breach has occurred, by sending electronic notification through the link at <http://www.fcc.gov/eb/CPNI/> to the central reporting facility, which will then notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI).

We understand that we may not notify customers or the public of the breach earlier than seven (7) days after we have notified law enforcement through the central reporting facility. If we wish to notify customers or the public immediately, where we feel that there is "an extraordinarily urgent need to notify" to avoid "immediate and irreparable harm," we inform law enforcement of our desire to notify and comply with law enforcement's directions.

Records relating to such notifications are kept in accordance with our record-keeping policies. These records include: (i) the date we discovered the breach, (ii) the date we notified law enforcement, (iii) a detailed description of the CPNI breached, and (iv) the circumstances of the breach.

During the course of the year, we compile information regarding pretexter attempts to gain improper access to CPNI, including any breaches or attempted breaches. We include this information in our annual CPNI compliance certification filed with the FCC.

Signed

A handwritten signature in black ink, reading "Thomas J. Brochin", is written over a horizontal line. The signature is cursive and fluid, with the first name "Thomas" and last name "Brochin" clearly legible.