CONFIDENTIAL

CPNI Compliance Policy of EASTON UTILITIES

Effective September 15, 2008

The following summary describes EASTON UTILITIES' policies that are designed to protect the confidentiality of Customer Proprietary Network Information ("CPNI") and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C.F.R. Part 64, Subpart U, Section 64.2001 *et seq*. CPNI is (a) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (b) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

EASTON UTILITIES trains employees on the limitations of use or disclosure of CPNI as governed by federal law and EASTON UTILITIES' policy. EASTON UTILITIES' policy, administered by its CPNI Compliance Manager, Ted Book, Director of Cable & Communications, establishes the procedures and safeguards regarding EASTON UTILITIES' use and disclosure of CPNI set forth below.

Because the details of this policy could provide a roadmap for unauthorized persons to attempt to subvert these policies and attempt to obtain CPNI, copies of this policy and related training materials are classified as confidential and may be provided only to EASTON UTILITIES' employees or to parties approved by the CPNI Compliance Manager. Notwithstanding the foregoing, EASTON UTILITIES employees may discuss the requirements of these policies with customers and prospective customers as appropriate in the ordinary course of business.

I. USE OF, DISCLOSURE OF, AND ACCESS TO CPNI

EASTON UTILITIES will use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including the publishing of directories; to initiate, render, bill and collect for communications services; to protect the rights or property of EASTON UTILITIES, or to protect users or other carriers or service providers from fraudulent or illegal use of, or subscription to, such services; to market services within the categories of services to which the customer already subscribes; to provide inside wiring installation, maintenance, or repair services; as required by law; or as authorized by the customer.

Except as provided above, EASTON UTILITIES does not use CPNI to market services. EASTON UTILITIES has established a supervisory review process regarding its compliance with the FCC's CPNI rules for outbound marketing situations and maintains records of carrier compliance for a minimum period of one year. In the event that any employee or agent wishes to use CPNI for marketing for which customer approval is required, such proposed use is subject to a supervisory review process that shall involve a supervisor designated by the senior employee

responsible for marketing or the CPNI Compliance Manager. If such use is approved, EASTON UTILITIES shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

EASTON UTILITIES does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Above and beyond the specific FCC requirements, EASTON UTILITIES will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. All EASTON UTILITIES Customer Service Representatives (CSRs) are trained in these procedures. The training emphasizes, among other points, that CSRs be cognizant that unauthorized persons may have significant apparent familiarity with a customer's biographical and account information.

The FCC's rules require EASTON UTILITIES on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting." If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to EASTON UTILITIES' existing policies that would strengthen protection of CPNI, they should report such information immediately to EASTON UTILITIES' CPNI Compliance Manager so that EASTON UTILITIES may evaluate whether existing policies should be supplemented or changed.

A. Inbound Calls to EASTON UTILITIES Requesting CPNI

CSRs may not disclose any CPNI to an inbound caller until the caller's identity has been authenticated. For CPNI not including Call Detail Information (CDI), CSRs authenticate callers by requesting their telephone number, account number, name and address.

CDI includes any information that pertains to the transmission of specific telephone calls, including, for outbound calls, the number called, and the time, location, or duration of any call and, for inbound calls, the number from which the call was placed, and the time, location, or duration of any call.

EASTON UTILITIES' CSRs do not reveal any Call Detail Information (CDI) to inbound callers. The CSRs that answer inbound telephone calls do not have access to CDI. If a caller requests CDI from the past 30 days, EASTON UTILITIES' CSRs will ordinarily first encourage the caller to obtain the requested information from the customer's online account. If the caller is unable or not interested to obtain the information from their online account, or if the requested CDI pertains to a time period prior to prior to 30 days, the CSR shall forward the request to the EASTON UTILITIES personnel that have access to CDI. EASTON UTILITIES' ordinary policy is to provide the requested CDI by sending the information by mail to a mailing address of record for the account, but only if such address has been on file with EASTON UTILITIES for at least 30 days. Letters providing CDI to a customer will instruct the customer that any further

questions about this information must be submitted in writing. In the event that a customer has changed their address within the prior 30 days, or for appropriate circumstances, EASTON UTILITIES may discuss CDI with a customer on the phone, but only in a call initiated by EASTON UTILITIES and placed to the customer's telephone number of record.

B. Online Accounts

EASTON UTILITIES' customers may obtain certain telephone account information from two online sources accessed from the EASTON UTILITIES website. To access either of these on-line accounts, the customer must enter a login ID that they create and a password established in accordance with the criteria set forth below.

The first online portal, EASTON UTILITIES' billing portal, provides customers with online access to their consolidated cable, broadband and telephone bills, and permits them to view and pay their bill. The second portal, the Call Detail portal, permits customers to view CDI from calls within the past 30 days and some other CPNI, such as the amount of their telephone bill.

Shortly before the effective date of this policy, all of EASTON UTILITIES' Call Detail online access accounts for which the customer had not created a password were locked such that they could not be accessed without the entry of a new randomly-generated password that the customer must obtain from EASTON UTILITIES. Similarly, the billing portal was changed so that a user could not create a new account without entering a new randomly-generated Personal Identification Number (PIN) that the customer must obtain from EASTON UTILITIES. Because these passwords and PINs will be generated randomly, they are not expected to include any material portion of the customer's account number, telephone number, street address, zip code, social security number, date of birth, or other biographical or account information.

When a customer attempts to log in to a Call Detail online account and is prompted for a password, if they do not know or have forgotten their login ID and/or password, the customer may contact EASTON UTILITIES to request that their login ID and/or password be mailed to the mailing address of record for their account.

The billing portal online site explains that new users must register to establish a login and password. To register, customer must enter their account number, EASTON UTILITIES PIN, telephone number and zip code. The site instructs them that if they have not obtained or do not know their EASTON UTILITIES PIN, they should contact EASTON UTILITIES to request that their login ID and/or password be mailed to the mailing address of record for their account.

Upon receipt of requests for a Call Detail password or billing portal PIN, EASTON UTILITIES will mail the requested information to the address of record if such address has been on file for at least 30 days. If the street address on file has been entered within 30 days, or if a customer indicates an urgent need to access an on-line account, EASTON UTILITIES may provide a login ID, password or PIN to a customer by placing a telephone call to the customer's telephone number of record. EASTON UTILITIES personnel with access to PINs and passwords are trained that they may not distribute passwords except in conformance with these requirements,

including a specific instruction that under no circumstances may they disclose a PIN or password to an inbound caller.

Customers are permitted to change their password on the billing portal after they have logged in by providing their existing password. Both portals instruct the user that passwords should not consist of any portion of their account number, telephone number, street address, zip code, social security number, date of birth, words, or easily-guessed strings of characters.

When a customer registers their account on the online billing portal, after the correct entry of their PIN, they are required to enter an email address of record for their account.

If a customer forgets the login or password they have established for the online billing portal, they are given the option to have their login and password emailed to their email address of record. If they cannot access their email account, as an alternative they may click a link to reset their password. To reset a password, the user must enter their account number, EASTON UTILITIES PIN, telephone number and zip code. Upon successful entry of this information, the site will provide the login ID and will permit the user to create a new password.

C. In-Person Disclosure of CPNI at EASTON UTILITIES Offices

EASTON UTILITIES may disclose CPNI to a customer visiting a EASTON UTILITIES office if they present a valid photo ID matching the customer's account information. A "valid photo ID" is a government-issued means of personal identification with a photograph such as a driver's license, passport, or comparable ID that is not expired.

D. Notice of Account Changes

When an online account is created (except at initiation of service) or when a password or PIN is changed, EASTON UTILITIES will mail a letter to customer's address of record notifying them of the change. When an address of record is changed (except at initiation of service), EASTON UTILITIES will send a notice to customer's former address of record notifying them of the change. The notice(s) provided under this paragraph will direct the customer to notify EASTON UTILITIES if they did not authorize the change.

E. Business Customer Exemption

The authentication requirements for disclosure of CPNI do not apply to disclosure of business customer information by a dedicated account representative who knows through personal experience that the person requesting the information is authorized representative of the customer and that the contract between EASTON UTILITIES and that business customer specifically addresses the protection of CPNI.

F. Audit Trail

EASTON UTILITIES employees must use a unique login and password to obtain access to databases that include CPNI. All instances of each employee access to a customer account are logged and the logs are maintained for a reasonable time. Company accordingly has access to an

audit trail of all such access that shall be consulted in the event that a breach of a customer's CPNI is detected. In any instance where a EASTON UTILITIES employee discloses CPNI to a party other than the customer, or CDI to the customer, they must enter a notation into the log associated with the customer account describing the CPNI disclosed, the means of disclosure and the identity of the party to which the information was provided.

G. Data Retention

Online accounts do not provide access to CDI that is older than approximately 30 days.

EASTON UTILITIES destroys customer information that is no longer necessary for the purpose for which it is collected unless there is a legitimate request or order to inspect the information still outstanding or the information remains in routine records that are periodically discarded under the company's document retention policies. The information that customers have provided to EASTON UTILITIES upon installation of service is maintained in management information system and billing systems, and is updated as new information is added. Accounting and billing records are retained for ten years for tax and accounting purposes or until the relevant income tax years for which the document was created have been closed for income tax purposes and/or all appeals have been exhausted. Routine paper records necessary to render, or conduct legitimate business activities related to the service provided customers are kept in accordance with EASTON UTILITIES's document retention program. Paper records such as work orders and records of technical maintenance and service are retained for three years. These records may remain on file even after a customer has terminated service. Subject to applicable law, records relating to involuntary disconnects are kept indefinitely to facilitate collection and evaluation of credit worthiness and are updated as new information is added.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Federal law imposes very specific requirements upon EASTON UTILITIES in the event that we become aware of any breach of customer CPNI. A breach includes any instance in which any person has intentionally gained access to, used, or disclosed a EASTON UTILITIES customer's CPNI beyond their authorization to do so. Any EASTON UTILITIES employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the EASTON UTILITIES CPNI Compliance Manager. Such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer or any member of the media, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

EASTON UTILITIES' CPNI Compliance Manager is Ted Book who may be contacted at 410-763-9477 or tbook@eucmail.com.

It is EASTON UTILITIES' policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to our customers, to make any adjustments as needed to prevent a recurrence of the breach, and to alert

law enforcement promptly. Therefore, although employees who violate EASTON UTILITIES' CPNI policies are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If an EASTON UTILITIES employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to EASTON UTILITIES' CPNI Compliance Manager who will determine whether to report the incident to law enforcement. EASTON UTILITIES' Compliance Manager will also determine whether it is appropriate to update EASTON UTILITIES' CPNI policies or training materials in light of the new information.

B. Notification Procedures

As soon as practicable, and in no event later than seven (7) business days upon learning of a breach, the EASTON UTILITIES CPNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: http://www.fcc.gov/eb/cpni. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450) for instructions.

EASTON UTILITIES will not under any circumstances, except as provided below, notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI. (A full business day does not count a business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure.

If EASTON UTILITIES receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach. We are not required to inform customers whose CPNI was not actually disclosed.

EASTON UTILITIES will delay notification to customers or the public upon request of the FBI or USSS.
If the EASTON UTILITIES Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; EASTON UTILITIES still may not notify customers sooner unless given clearance to do so from *both* the USSS and the FBI.

IV. RECORD RETENTION

The EASTON UTILITIES Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

EASTON UTILITIES maintains a record, for a period of at least one year, of: those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI; in which CPNI is used to market services within the package of services to which the customer already subscribes; and of supervisory review of marketing that proposes to use CPNI or to request customer approval to disclose CPNI.

EASTON UTILITIES maintains a record for at least two years of all customer complaints related to their handling of CPNI, and records of EASTON UTILITIES' handling of such complaints. The CPNI Compliance Manager will assure that all complaints are reviewed and that EASTON UTILITIES considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

EASTON UTILITIES will have an authorized corporate officer, as an agent of the company, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that EASTON UTILITIES has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explain how EASTON UTILITIES's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions may be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

EASTON UTILITIES employees must use a unique login and password to obtain access to databases that include CPNI. All employees with access to CPNI receive a copy of EASTON UTILITIES' CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, EASTON UTILITIES conducts mandatory CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, technical support personnel who field calls from customers, provisioning personnel who have access to and research customer inquiries regarding CDI, and marketing personnel. The CSR training emphasizes, among other points, that CSRs be cognizant that some unauthorized persons may have significant apparent familiarity with a customer's biographical and account information.