BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI

In the Matter of the Establishment of a Working Case for the Writing of a New Rule on the Treatment of Customer Information by Commission Regulated Electric, Gas, Steam Heating, Water, and Sewer Utilities and Their Affiliates and Nonaffliliates	))))))	Case No. AW-2018-0393

THE OFFICE OF THE PUBLIC COUNSEL'S COMMENTS

COMES NOW the Office of the Public Counsel (OPC), by and through counsel, and for its Comments states as follows:

BACKGROUND

On July 11, 2018, the Public Service Commission (Commission) established Case No. AW-2018-0393 in response to the Commission Staff's (Staff) Motion to Open Rulemaking Workshop. The Commission Staff acted pursuant to Executive Order 17-03 to consolidate existing rules, and accordingly proposed new rules regarding the sharing of customer information by Commission regulated utilities.

The Commission requested comments regarding the Staff's drafted rules to be submitted by no later than August 10, 2018. The comment period was later extended to August 24, 2018. As the OPC is charged to "represent and protect the interests of the public", the OPC offers comments as follows.[1]

POSITION ON THE SHARING OF CUSTOMER INFORMATION GENERALLY

The OPC is extremely cautious of any proposed rule enabling the free exchange of customer information without customer consent. The customer information that public utilities have access to is extremely intimate can be revealing as to our daily habits and constitutionally

[1] Section 386.710, RSMo (1977).

protected activities. The late Justice Antonin Scalia bemoaned the travesty that would occur if information regarding "at what hour each night the lady of the house takes her daily sauna and bath" was acquired with her consent.[2] Utilities are particularly situated to have access to information regarding Justice Scalia's proverbial matriarch. Therefore, particular esteem should be paid to protecting utility customer information. Most customer data should accordingly be presumed non-shareable except in limited instances required for the furnishing of utility services or via customer consent. The OPC believes this position is reasonable given its implementation in multiple jurisdictions.[3]

A default position of securing customer data is especially warranted when recent events have garnered an exceedingly focused public anxiety on privacy issues. One need only perform a cursory internet search to learn about notable customer data breaches from Equifax,[4] Yahoo,[5] and Uber[6] to name only a few examples. Revelations of Russian hackings of Democrat servers have also potentially forever diminished the public's confidence in their representative government.[7]

---

[2] *Kyllo v. United States*, 533 U.S. 27, 38 (2001).

[3] *See* Cal. Pub. Util. Code § 8380 (2012) ("An electrical corporation or gas corporation shall not share, disclose, or otherwise make accessible to any third party a customer's electrical or gas consumption data, except as provided in subdivision (e) [of this section] or upon the consent of the customer"); *see also* D.C. Code § 8-1774.07 (2016) ("The [sustainable energy utility] shall not sell or otherwise disclose any customer or billing information to any third party without express written authorization from the customer"); Wash. Admin. Code § 480-100-153 (2001) ("An electric utility may not disclose or sell private consumer information with or to its affiliates, subsidiaries, or any other third party for the purposes of marketing services or product offerings to a customer who does not already subscribe to that service or product, unless the utility has first obtained the customer's written or electronic permission to do so").

[4] Alex Johnson, *Equifax Breaks Down Just How Bad Last Year's Data Breach Was*, NBC NEWS, May 8, 2018, https://www.nbcnews.com/news/us-news/equifax-breaks-down-just-how-bad-last-year-s-data-n872496 (detailing the unauthorized access of 146.6 million Social Security numbers by hackers).

[5] Selena Larson (1), *Every Single Yahoo Account was Hacked – 3 Billion in All*, CNN, Oct. 4, 2017, https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html (relating to a data breach of all of Yahoo's users that was not disclosed for four years).

[6] Selena Larson (2), *Uber's Massive Hack: What We Know*, CNN, Nov. 23, 2017, https://money.cnn.com/2017/11/22/technology/uber-hack-consequences-cover-up/index.html (recounting how Uber had paid a $100,000 ransom to hackers for its user data, including 600,000 driver's license numbers, to be returned without informing regulators).

[7] *See* Devlin Barrett & Matt Zapotsky, *Mueller Probe Indicts 12 Russians with Hacking of Democrats in 2016*, WASHINGTON POST, July 13, 2018, https://www.washingtonpost.com/world/national-security/rod-rosenstein-expected-to-announce-new-indictment-by-mueller/2018/07/13/bc565582-86a9-11e8-8553-

Missouri consumers are acutely aware of the potential customer information breaches of utilities given that two of their major utility service providers had unauthorized breaches within the past year.[8]

With these recent customer information security failings in mind, it becomes apparent that even the existing safeguards of customer information cannot be completely protected. The advancing nature of technology and security risks require ever vigilance. What security customers have is then further curtailed by their public utility freely divulging sensitive information to affiliate and nonaffliate parties. Each time that a utility contracts with a third-party, the potential privacy concerns and potential harms are compounded because the number of chances for exposure increases exponentially.[9]

POSITION ON DEFINITIONS OR LACK THEREOF FOR CERTAIN TERMS

The OPC also believes that several terms used through the proposed rule need to be further defined to alleviate confusion and to protect consumers. The OPC is specifically troubled by the drafted definition of "customer information" that would be permissibly shared under the proposed rule. The current definitional list explicitly includes certain sharable customer data, but then also provides that the list is not exhaustive. At the outset, the OPC recommends that the definition of "customer information" be narrowly drafted so as to include what information may be necessary for safe and adequate service, while also securing against future developed information that could be shared, unwittingly or otherwise, to the detriment of consumers. The utilities included in this

a3ce89036c78_story.html?utm_term=.0b41f4b91675 (reporting on the indictment of twelve Russian military officers on charges of hacking Democrat computers).

[8] *See Potential Data Breach at Authorized Payment Locations*, KANSAS CITY POWER & LIGHT, https://www.kcpl.com/involvement/safety/fraud-alerts/potential-data-breach-at-authorized-payment-locations (last visited July 16, 2018) (admitting the unauthorized release of customer information by a contracted entity); *see also* Charles Pyatt, *City Utilities Discloses Possible Data Breach*, FOX 5 NEWS, Mar. 30, 2018, http://www.fox5krbk.com/story/36974808/city-utilities-discloses-possible-data-breach (detailing the breach of Springfield Utilities customer data).

[9] *Direct Testimony of Geoff Marke*, Case Nos. ER-2018-0145, ER-2018-0146 (Jun. 19, 2018).

working case should be able to honestly provide a comprehensive list of necessarily shareable customer information, and thus a liberally constructed definition is unjustified.

The components of "customer information" given by the proposed rule are also troubling. The drafted definition lists social security numbers, utility service usage, driver's license number, medical information, and health insurance information data as transmittable customer information. It is not readily apparent why social security numbers, driver's license numbers, or health insurance details should ever be shared by a public utility under authority by Commission rule. None of that information needs to be shared to address bad debt or collections, and none of this data pertains to utility services. Under the exercise of due caution, only that customer information which is necessary for utility business operations should be shared either through customer consent or not. In addition, considering that public utilities have begun providing their own insurance programs, a public utility being permitted to share a customer's health insurance particulars could easily be an affiliate transaction violation in the future as utility parent companies continue to diversify their portfolios.[10]

The terms "medical information" and "financial account" are undefined and too vague as drafted in the definition of "customer information" under subdivision (B) of subsection (1). It is not clear whether medical information pertains only to information surrounding persistent health conditions that require uninterrupted utility service, or other identifiable information that could expose consumers to embarrassment or harm. Considering also that the federal Health Insurance Portability and Accountability Act does not allow nonconsensual customer information distribution because of similar concerns over harm and mortification, the OPC recommends that Commission approved rules at a minimum exclude personally identifiable information from

[10] *See Easy, Affordable Home Protection*, AMERICAN WATER RESOURCES, https://awrusa.com/products-services (last visited July 16, 2018) (advertising various insurance packages).

"medical information."[11] As for "financial account" it is not clear whether this term refers only to the personal account that a customer may have with a public utility or the credit card and checking account access information connected to that account as well. Absent compelling evidence why a utility should be able to share such intimate financial information this interpretation should be definitionally excluded as well.

Subdivision (A) of subsection (2) of the proposed rule provides that consumer information may be shared without prior content in instances where "when any covered utility contracts with an affiliate or a third party nonaffiliated to perform a utility related service." The phrase "utility related service" should be defined so as limit those cases where customer information is exposed. Without a refining definition the phrase may be so broadly interpreted as to encompass tangentially related business just because a public utility or its affiliate is involved. Consideration should again be paid to the ever expanding library of products and services offered by utility parent and affiliate companies.

Likewise, the phrase "immaterial amount" is not properly elucidated when used in subdivision (A) of subsection (5) of the proposed rule. The subject language provides that public utilities need only disclose a breach of customer data if "more than an immaterial amount" has been exposed. Whether or not information is "immaterial" is largely subjective and may be contextually dependent. A little amount of information on a vast array of consumers may be deemed "immaterial," but so could a lot of information on only one customer relative to the plethora of consumers not affected. Of course the latter situation would not considered immaterial by the harmed individual. "Immaterial" amount should be properly defined so as to convey intent and avoid conflicting interpretations.

[11] *See* 110 Stat. 1936 (1996).

POSITION ON CUSTOMER PRIVACY STATEMENT

The OPC believes that a customer privacy statement is a necessary step for public utilities to take in order to instill public confidence and to better inform utility customers of what information may or may not be shared by their utility. The OPC imagines that a privacy statement would be a set of practices employed by a utility along with stated principles, and that the privacy statement would then be prominently displayed on the utility's publically available website. However, the OPC decided to leave the definition as "TBD" or "to be determined," deferring instead to stakeholder input.

POSITION ON THE REQUISTE CONTRACTS TO SHARE CUSTOMER INFORMATION WITHOUT CUSTOMER CONSENT

The proposed rule's requisite contracts for the sharing of customer information without consumer consent are contrary to the OPC's position on customer data, and have insufficient transparency and oversight controls. Within section (2) the proposed rule requires that contracts between utilities and third parties declare that customer information is "the sole property of the covered utility." If customer information is deemed to be the property of utilities by Commission rule, then arguably utilities may then capitalize upon that property as they see fit. Customers may then have no right to have their prior records deleted. The OPC believes that it is in the best interest of captive rate payers to not consider their information to be a property interest solely of their utility, and for the Commission to preserve their right to erasure.[12]

The proposed rule also enumerates certain required parts of the contracts between utilities and third parties, but fails to account for enforcement or transparency. The rules do specify whether

[12] The security interest in having records of oneself be erased has gained notable acceptance in the international community as evidenced by recent European Union standards. *See* General Data Protection Regulation Art. 17, Regulation (EU) 2016/679, *available at* https://gdpr-info.eu/art-17-gdpr/.

or not the contracts are filed with the Commission for approval, or whether the OPC may challenge them. The OPC recommends the affirmative in the prior two instances.

POSITION ON THE LACK OF ENFORECMENT PROVISIONS IN THE PROPOSED RULE

The proposed rules should include enforcement and penalty provisions. As previously discussed, the proposed rule requires certain contractual terms for the sharing of customer data without consumer consent, but does not specify enforcement procedures nor does it include participation by the OPC. This deficiency persist throughout the rule's other sections. In order to ensure compliance and safeguard consumers, the OPC recommends that the OPC be explicitly referenced as an interested party in the rule, and that any utility activity related to a material data breach be deemed imprudent. Similar to how a superseding intervening tortious act stops a chain of reasonably prudent behavior, actions by a utility or its contracted third parties should not be borne by ratepayers once it is determined what action resulted in a breach of customer information.

POSITION ON THE PROCEDURES FOLLOWING THE VIOLATIONS OF THE PROPOSED RULE

The proposed rule's notification process following a violation of the rule fails to consider segmentation. Section (5) of the rule instructs utilities to inform the Commission of any more than immaterial amount of customer data that has become public or possessed by an unauthorized entity. However, this procedure does not contemplate a successive series of immaterial breaches that when considered together may amount to a material if not catastrophic unauthorized disclosure of captive ratepayer information. To rectify this situation the OPC recommends that customer data breaches be measured not just by materiality, but by frequency as well. Missouri customers should be just as informed about a multitude of questionable behavior just as they should about one material risk to their security.

POSITION ON THE WAIVER OF THE PROPOSED RULE

The proposed rule's traditional waiver provision is inappropriate for a rule safeguarding customer information and minimizing risk. The proposed rule contains a general waiver provision in section (6) requiring only for the showing of good cause for a waiver. Although good cause is a traditional standard for Commission rule variances, it is improper in this instance. The unauthorized release of one's data can be a mere inconvenience, or forever debilitate a customer's economic prospects and financial wellbeing.[13] Because a utility's actions can potentially result in life long repercussions for their captive ratepayers, the OPC believes that they should be held to a higher standard than "good cause" for the right to expose their customers to that risk. Utilities should instead present a compelling interest to the Commission for a variance or waiver.

Furthermore, the proposed rule's waiver section fails to indicate reporting or tracking procedures for a utility's actions to resume compliance with the rule. The OPC is concerned that a prior evaluation of good cause may in the future turn out to be less than good. If it turns out later that customer information did not need to be exposed, then the associated costs of the waiver should not be borne by ratepayers. The OPC recommends that proper tracking and sharing protocols be included in any waiver provision so that customer information may still be secured.

POSITION ON HOW TO PROCEED WITH RULEMAKING

The OPC recommends that other stakeholders and members of the public at large be invited to participate in the Commission's rulemaking process. Because of the sensitive nature of customer information security, and its recent prominence in the public discourse, the OPC requests that any subsequent rulemaking process regarding this proposed rule employ the use of local public

[13] Adam Shell, *Equifax Data Breach Could Create Lifelong Identify Theft Threat*, USA TODAY, Sep. 9, 2017, https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/.

hearings throughout Missouri, and invite other non-utility stakeholders. The Commission has historically performed local public hearings for rulemakings regarding sensitive and potentially controversial rulemaking such as when the fuel adjustment clause rules were formally codified.[14] If a highly technical financial mechanism was deserving of multiple avenues for the public to voice their concerns because of the creation of a surcharge, surely the public should be involved in any proposed rule regarding their own data and security.

WHEREFORE, the OPC respectfully submits its Comments.

Respectfully,

OFFICE OF THE PUBLIC COUNSEL

/s/ Caleb Hall
Caleb Hall, #68112
Senior Counsel
200 Madison Street, Suite 650
Jefferson City, MO 65102
P: (573) 751-4857
F: (573) 751-5562
Caleb.hall@ded.mo.gov

Attorney for the Office of the Public Counsel

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing was served, either electronically or by hand delivery or by First Class United States Mail, postage prepaid, on this 24th day of August, 2018, with notice of the same being sent to all counsel of record.

/s/ Caleb Hall

[14] *E.g., Notice Regarding Public Hearing*, Case No. EX-2006-0472 (Aug. 7, 2006).

4 CSR 240-10.XXX Customer Information of Electrical Corporations, Gas Corporations, Heating Companies, Water Corporations and Sewer Corporations

PURPOSE: Strong consumer data privacy protections are essential to maintaining the trust of ratepayers. This rule is intended to prevent the misuse and inadvertent disclosure of customer information. All matters regarding treatment of customer information and release of specific customer information to an affiliate or a third party nonaffiliate respecting the provision of utility related services may occur without customer consent but must be a matter of written contract between the regulated electrical corporation, gas corporation, heating company, water corporation and sewer corporation (covered utility) and the affiliate or third party nonaffiliate pursuant to the conditions set out in the rule below. All matters regarding treatment of customer information and release of specific customer information to an affiliate or a third party nonaffiliate respecting the provision of a nonutility related service, or other service not regulated by the commission, must be limited to situations where there is documented recorded or written customer consent and a written contract between the covered utility and the affiliate or the third party nonaffiliate.

(1) Definitions

(A) Aggregate~~d~~ data means a combination of data elements for multiple customers to create a data set that is sufficiently anonymous so that it does not reveal the identity of an individual customer.

(B~~A~~) Covered utility means, for purposes of this rule, an electrical corporation, gas corporation, heating company, water corporation, or sewer corporation as defined in section 386.020, RSMo., and subject to commission regulation pursuant to Chapters 386 and 393, RSMo.,

(C) Critical customer information means a subset of information regarding customers in general, including, but not limited to, one or more of the following items of one or more customers on the system of a covered utility that is identifiable with one or more particular customers: birth date, social security number, driver's license number, health insurance information, credit reporting information, internet protocol address, bankruptcy or probate information, and demographic data including race; religion; sexual orientation or self-identification; nationality; and immigration status.

(D) Customer privacy statement means TBD.

(E) Customer Usage Data means customer specific electric, gas and water usage data, including but not limited to ccf, Mcf, therms, dth, kW, kWh, voltage, var, power factor or gallons and other information that is recorded by the electric, gas and water meter for the covered utility and stored in its system.

(F) Financial account means a covered utility created account used for the tracking of billing and payments of a particular customer or account, except that the term shall not include critical customer information.

(G) Immaterial amount means that information discoverable in a professional or social register.

(H) Medical information means only that information related to a particular diagnosis or condition necessitating uninterrupted utility service.

(I) Nonutility related service means those functions not directly connected to the furnishing of electricity, gas, heat, water, or sewer services including, but not limited to, services not regulated by the commission and demand-side programs under Section 393.1075, RSMo.

(~~J~~B) Primary ~~C~~customer information means a subset of information regarding customers in general, ~~and includes~~ including ~~but is not limited to~~ one or more of the following items of one or more customers on the system of a covered utility that is identifiable with one or more particular customers: name, address, phone number, ~~social security number, utility service usage,~~ payment history, and financial account, ~~driver's license number, medical information, and health insurance information~~. Customer information includes information provided to a covered utility by an affiliated or nonaffiliated third party person, entity, or association.

(J) Privacy impact assessment means an evaluation ensuring conformance with applicable legal, regulatory, and policy requirements for privacy; determining risks and effects; and evaluating protections and alternative processes to mitigate potential privacy risks.

Commented [HC1]: Based on the DHS definition.

(K) Secondary customer information means a subset of information regarding customers in general, including one or more of the following items of one or more customers on the system of a covered utility that is identifiable with one or more particular customers: utility service usage, customer usage data, and medical information.

(L) Utility related service means regulated utility functions limited to the direct furnishing of electricity, gas, heat, water, or sewer service; billing; bad debt; repairs; discontinuation and continuation of service; grid maintenance; and any other activity provided in a commission-approved tariff except for those activities defined as a nonutility related service.

Commented [HC2]: Based on California's SB 1476

~~(C) Information means any data obtained by a covered utility that is not obtainable by nonaffiliated entities or can only be obtained at a competitively prohibitive cost in either time or resources.~~

(2) Utility Related Services

(A) When any covered utility contracts with an affiliate or a third party nonaffiliate to perform a utility related service on behalf of the covered utility and ~~specific~~ primary customer information to perform the utility related service is required, the covered utility ~~will~~ shall only provide the affiliate or third party nonaffiliate with the necessary ~~specific~~ primary customer information without customer consent under the following contractual terms:
1. The affiliate or third party nonaffiliate shall be directed that the ~~specific~~ primary customer information remains the sole property of the ~~covered utility~~customer;
2. The affiliate or third party nonaffiliate shall be authorized to use the ~~specific~~ primary customer information solely to perform the contracted for service;

3. The affiliate or third party nonaffiliate shall be expressly prohibited from any other use of the ~~specific~~ primary customer information with prohibitions to the affiliate or third party nonaffiliate set out in the contract for any unauthorized use of the specific customer information;
4. The affiliate or third party nonaffiliate shall be directed to treat the ~~specific~~ primary customer information as confidential at all times with specified prohibitions set out in the contract for not treating the ~~specific~~ primary customer information as confidential; and
5. The affiliate or third party nonaffiliate shall be directed to return to the covered utility, within ten (10) days following the receipt of a written request, all ~~specific~~ primary customer information provided to the entity with an attestation that all replication of the information has been returned to the covered utility or the affiliate or third party nonaffiliate may provide to the covered utility an attestation that the affiliate or third party nonaffiliate has destroyed or has had destroyed all material identifying the ~~specific~~ primary customer information.

(3) Nonutility Related Services
(A) When an affiliated or nonaffiliated third party person or entity contracts with the covered utility to perform a nonutility related service and that particular service requires primary or secondary specific customer information, the ~~regulated electrical corporation, gas corporation, heating company, water corporation, or sewer corporation will~~covered utility shall only provide that affiliate or third party nonaffiliate with ~~specific~~ primary or secondary customer information ~~only~~ with documented recorded or written customer consent, or by Commission order.
(B) When a covered utility provides a nonutility related service and that particular service requires primary or secondary customer information, the covered utility shall first receive documented recorded or written customer consent to use that primary or secondary customer information before providing that service, except as otherwise provided in subdivision (A) of this subsection.
(C) A covered utility shall not provide or sell primary or secondary customer information with its affiliates or nonaffiliate third-parties for the purposes of marketing services or product offerings to a customer who does not already subscribe to that service or product, unless the utility has first obtained the customer's documented recorded or written consent to the contrary.

(4) Customer Data Privacy Policy
(A) Each covered utility shall file with the commission, for the commission's approval, a customer data privacy tariff that contains a customer data privacy policy. The privacy policy shall:
1. Clearly define customer information or data that the utility collects, maintains and for how long it will be maintained;
2. Protect all customer information collected for the covered utility from unauthorized use or disclosure by the covered utility, its affiliates, or contractors;
3. Ensure that, for secondary purposes, customer usage data, personally identifiable information, and certain other customer information are only disclosed to third parties with the customer's explicit consent;
4. Permit a customer to share his or her information with a third party that is not affiliated with the utility;

Commented [HC3]: Based on California's SB 1476.

Commented [HC4]: Based on Washington 480-100-153

5. Provide clear instructions regarding the method by which a customer and a third party, authorized by the customer, may obtain customer usage data in timely manner and a readily accessible format from the utility;
6. Indicate that the policy does not apply to aggregate data, containing general characteristics of a customer group, which is used for analysis, reporting, or program design purposes; and
7. The privacy policy shall be posted on the utility's website in a prominent position.
(B) Within six (6) months following the codification of these rules, covered utilities shall meet with commission staff and the office of the public counsel to solicit feedback and comments on the customer rights statement and privacy impact assessment.

(~~4~~5) Critical Customer Information
(A) A covered utility shall not provide or sell critical customer information to its affiliates or nonaffiliate third-parties for any purpose.

(6) Customer Consent
(A) For the purposes of this rule, customer consent shall be deemed documented recorded or written when a customer provides an affirmative response to a request to share his or her customer information on a commission approved form or recording.
(B) Customer consent shall only be deemed to have been offered for discrete requests or transactions, and shall not be inferred for ongoing or successive transactions.
(C) A Customer can withdraw his or her consent at any time.

(7) Advanced Metering
(A) A covered utility utilizing advanced metering infrastructure that allows a customer to access the customer's electrical consumption data shall enable the customer with the option to access that data without being required to agree to the sharing of his or her personally identifiable information, including electrical consumption data, with a third party.
(B) A covered utility shall use reasonable security procedures and practices to protect a customer's unencrypted electrical consumption data from unauthorized access, destruction, use, modification, or disclosure, and prohibit the use of the data for a secondary commercial purpose not related to the primary purpose of any contract under subsection (2) of this section without the customer's consent.

Commented [HC5]: Based on California's SB 1476

(8) ~~General or~~ Aggregated Customer Information
~~(A) General or~~ and ~~aggregated customer information shall be made available to affiliates or third party nonaffiliates upon similar terms and conditions.~~
(A) When sharing or disclosing aggregate customer information on residential customers a covered utility shall include at least fifteen (15) customers with no customer's load exceeding fifteen (15) percent of the data included in the aggregate.
(B) When sharing or disclosing aggregate customer information on nonresidential customers a covered utility shall include at least four (4) customers with no customer's load exceeding eighty (80) percent of the data included in the aggregate.

(9~~5~~) Notification to Commission of Violations of Rule
(A) If a covered utility becomes aware of more than an immaterial amount of its ~~confidential~~ customer information having become public or passed into the possession of an unauthorized entity in any single instance, the covered utility shall notify the staff counsel's office and public counsel within one day of knowledge of the customer information breach ~~as soon as it has verified that this has occurred~~. Notice of the customer information becoming public or having been passed into the possession of an unauthorized entity shall be included with all affected customer's bills on a commission approved form.
(B) If a covered utility becomes aware of more than an immaterial amount of its customer information having become public or passed into the possession of an unauthorized entity at least four times in any calendar year, the covered utility shall notify the staff counsel's office and public counsel upon the fourth breach of customer information. Notice of the customer information becoming public or having been passed into the possession of an unauthorized entity shall be included with all customer's bills on a commission approved form.

(10) Enforcement
(A) When enforcing these standards, or any order of the commission regarding these standards, the commission may apply any remedy available to the commission.
(B) Any activity by a covered utility related and incident to a violation of this rule, including more than an immaterial amount of its customer information becoming public or passed into the possession of an unauthorized entity, shall be deemed imprudent and is not recoverable.

(11~~6~~) Waiver
(A) Provisions of this rule may be waived by the Commission ~~for good cause shown~~ for compelling cause shown after an opportunity for a hearing.
(B) If approved by the commission, the covered utility shall inform all affected customers of the waiver on a separate commission approved disclosure on each customer's bill.
(C) Within six months following the commission's order for a waiver, the covered utility shall file a report and accompanying documentation on the provision of specific customer information with the commission. Such report may be included within the covered utility's customer information security plan under subsection (10) of this section.

(12) Exception
(A) Nothing in 4 CSR-10.XXX precludes a covered utility from providing specific customer information without documented recorded or written customer consent when such provision is pursuant to state or federal law or under an order of the commission.
(B) Nothing in this section shall preclude a covered utility from using customer aggregate data for analysis, reporting, or program management if all information has been removed regarding the individual identity of a customer.

4 CSR 240-10.XXX Customer Information of Electrical Corporations, Gas Corporations, Heating Companies, Water Corporations and Sewer Corporations

PURPOSE: Strong consumer data privacy protections are essential to maintaining the trust of ratepayers. This rule is intended to prevent the misuse and inadvertent disclosure of customer information. All matters regarding treatment of customer information and release of specific customer information to an affiliate or a third party nonaffiliate respecting the provision of utility related services may occur without customer consent but must be a matter of written contract between the regulated electrical corporation, gas corporation, heating company, water corporation and sewer corporation (covered utility) and the affiliate or third party nonaffiliate pursuant to the conditions set out in the rule below. All matters regarding treatment of customer information and release of specific customer information to an affiliate or a third party nonaffiliate respecting the provision of a nonutility related service, or other service not regulated by the commission, must be limited to situations where there is documented recorded or written customer consent and a written contract between the covered utility and the affiliate or the third party nonaffiliate.

(1) Definitions

(A) Aggregate data means a combination of data elements for multiple customers to create a data set that is sufficiently anonymous so that it does not reveal the identity of an individual customer.

(B) Covered utility means, for purposes of this rule, an electrical corporation, gas corporation, heating company, water corporation, or sewer corporation as defined in section 386.020, RSMo., and subject to commission regulation pursuant to Chapters 386 and 393, RSMo.,

(C) Critical customer information means a subset of information regarding customers in general, including, but not limited to, one or more of the following items of one or more customers on the system of a covered utility that is identifiable with one or more particular customers: birth date, social security number, driver's license number, health insurance information, credit reporting information, internet protocol address, bankruptcy or probate information, and demographic data including race; religion; sexual orientation or self-identification; nationality; and immigration status.

(D) Customer privacy statement means TBD.

(E) Customer Usage Data means customer specific electric, gas and water usage data, including but not limited to ccf, Mcf, therms, dth, kW, kWh, voltage, var, power factor or gallons and other information that is recorded by the electric, gas and water meter for the covered utility and stored in its system.

(F) Financial account means a covered utility created account used for the tracking of billing and payments of a particular customer or account, except that the term shall not include critical customer information.

(G) Immaterial amount means that information discoverable in a professional or social register.

(H) Medical information means only that information related to a particular diagnosis or condition necessitating uninterrupted utility service.

(I) Nonutility related service means those functions not directly connected to the furnishing of electricity, gas, heat, water, or sewer services including, but not limited to, services not regulated by the commission and demand-side programs under Section 393.1075, RSMo.

(J) Primary customer information means a subset of information regarding customers in general, including one or more of the following items of one or more customers on the system of a covered utility that is identifiable with one or more particular customers: name, address, phone number, payment history, and financial account, . Customer information includes information provided to a covered utility by an affiliated or nonaffiliated third party person, entity, or association.

(J) Privacy impact assessment means an evaluation ensuring conformance with applicable legal, regulatory, and policy requirements for privacy; determining risks and effects; and evaluating protections and alternative processes to mitigate potential privacy risks.

(K) Secondary customer information means a subset of information regarding customers in general, including one or more of the following items of one or more customers on the system of a covered utility that is identifiable with one or more particular customers: utility service usage, customer usage data, and medical information.

(L) Utility related service means regulated utility functions limited to the direct furnishing of electricity, gas, heat, water, or sewer service; billing; bad debt; repairs; discontinuation and continuation of service; grid maintenance; and any other activity provided in a commission-approved tariff except for those activities defined as a nonutility related service.

(2) Utility Related Services

(A) When any covered utility contracts with an affiliate or a third party nonaffiliate to perform a utility related service on behalf of the covered utility and primary customer information to perform the utility related service is required, the covered utility shall only provide the affiliate or third party nonaffiliate with the necessary primary customer information without customer consent under the following contractual terms:
1. The affiliate or third party nonaffiliate shall be directed that the primary customer information remains the sole property of the customer;
2. The affiliate or third party nonaffiliate shall be authorized to use the primary customer information solely to perform the contracted for service;
3. The affiliate or third party nonaffiliate shall be expressly prohibited from any other use of the primary customer information with prohibitions to the affiliate or third party nonaffiliate set out in the contract for any unauthorized use of the specific customer information;
4. The affiliate or third party nonaffiliate shall be directed to treat the primary customer information as confidential at all times with specified prohibitions set out in the contract for not treating the primary customer information as confidential; and

5. The affiliate or third party nonaffiliate shall be directed to return to the covered utility, within ten (10) days following the receipt of a written request, all primary customer information provided to the entity with an attestation that all replication of the information has been returned to the covered utility or the affiliate or third party nonaffiliate may provide to the covered utility an attestation that the affiliate or third party nonaffiliate has destroyed or has had destroyed all material identifying the primary customer information.

(3) Nonutility Related Services
(A) When an affiliated or nonaffiliated third party person or entity contracts with the covered utility to perform a nonutility related service and that particular service requires primary or secondary specific customer information, the covered utility shall only provide that affiliate or third party nonaffiliate with primary or secondary customer information with documented recorded or written customer consent, or by Commission order.
(B) When a covered utility provides a nonutility related service and that particular service requires primary or secondary customer information, the covered utility shall first receive documented recorded or written customer consent to use that primary or secondary customer information before providing that service, except as otherwise provided in subdivision (A) of this subsection.
(C) A covered utility shall not provide or sell primary or secondary customer information with its affiliates or nonaffiliate third-parties for the purposes of marketing services or product offerings to a customer who does not already subscribe to that service or product, unless the utility has first obtained the customer's documented recorded or written consent to the contrary.

(4) Customer Data Privacy Policy (A) Each covered utility shall file with the commission, for the commission's approval, a customer data privacy tariff that contains a customer data privacy policy. The privacy policy shall:
1. Clearly define customer information or data that the utility collects, maintains and for how long it will be maintained;
2. Protect all customer information collected for the covered utility from unauthorized use or disclosure by the covered utility, its affiliates, or contractors;
3. Ensure that, for secondary purposes, customer usage data, personally identifiable information, and certain other customer information are only disclosed to third parties with the customer's explicit consent;
4. Permit a customer to share his or her information with a third party that is not affiliated with the utility;
5. Provide clear instructions regarding the method by which a customer and a third party, authorized by the customer, may obtain customer usage data in timely manner and a readily accessible format from the utility;
6. Indicate that the policy does not apply to aggregate data, containing general characteristics of a customer group, which is used for analysis, reporting, or program design purposes; and
7. The privacy policy shall be posted on the utility's website in a prominent position.
(B) Within six (6) months following the codification of these rules, covered utilities shall meet with commission staff and the office of the public counsel to solicit feedback and comments on the customer rights statement and privacy impact assessment.

(5) Critical Customer Information
(A) A covered utility shall not provide or sell critical customer information to its affiliates or nonaffiliate third-parties for any purpose.

(6) Customer Consent
(A) For the purposes of this rule, customer consent shall be deemed documented recorded or written when a customer provides an affirmative response to a request to share his or her customer information on a commission approved form or recording.
(B) Customer consent shall only be deemed to have been offered for discrete requests or transactions, and shall not be inferred for ongoing or successive transactions.
(C) A Customer can withdraw his or her consent at any time.

(7) Advanced Metering
(A) A covered utility utilizing advanced metering infrastructure that allows a customer to access the customer's electrical consumption data shall enable the customer with the option to access that data without being required to agree to the sharing of his or her personally identifiable information, including electrical consumption data, with a third party.
(B) A covered utility shall use reasonable security procedures and practices to protect a customer's unencrypted electrical consumption data from unauthorized access, destruction, use, modification, or disclosure, and prohibit the use of the data for a secondary commercial purpose not related to the primary purpose of any contract under subsection (2) of this section without the customer's consent.

(8) Aggregated Customer Information
(A) When sharing or disclosing aggregate customer information on residential customers a covered utility shall include at least fifteen (15) customers with no customer's load exceeding fifteen (15) percent of the data included in the aggregate.
(B) When sharing or disclosing aggregate customer information on nonresidential customers a covered utility shall include at least four (4) customers with no customer's load exceeding eighty (80) percent of the data included in the aggregate.

(9) Notification to Commission of Violations of Rule
(A) If a covered utility becomes aware of more than an immaterial amount of its customer information having become public or passed into the possession of an unauthorized entity in any single instance, the covered utility shall notify the staff counsel's office and public counsel within one day of knowledge of the customer information breach. Notice of the customer information becoming public or having been passed into the possession of an unauthorized entity shall be included with all affected customer's bills on a commission approved form.
(B) If a covered utility becomes aware of more than an immaterial amount of its customer information having become public or passed into the possession of an unauthorized entity at least four times in any calendar year, the covered utility shall notify the staff counsel's office and public counsel upon the fourth breach of customer information. Notice of the customer information becoming public or having been passed into the possession of an unauthorized entity shall be included with all customer's bills on a commission approved form.

(10) Enforcement
(A) When enforcing these standards, or any order of the commission regarding these standards, the commission may apply any remedy available to the commission.
(B) Any activity by a covered utility related and incident to a violation of this rule, including more than an immaterial amount of its customer information becoming public or passed into the possession of an unauthorized entity, shall be deemed imprudent and is not recoverable.

(11) Waiver
(A) Provisions of this rule may be waived by the Commission for compelling cause shown after an opportunity for a hearing.
(B) If approved by the commission, the covered utility shall inform all affected customers of the waiver on a separate commission approved disclosure on each customer's bill.
(C) Within six months following the commission's order for a waiver, the covered utility shall file a report and accompanying documentation on the provision of specific customer information with the commission. Such report may be included within the covered utility's customer information security plan under subsection (10) of this section.

(12) Exception
(A) Nothing in 4 CSR-10.XXX precludes a covered utility from providing specific customer information without documented recorded or written customer consent when such provision is pursuant to state or federal law or under an order of the commission.
(B) Nothing in this section shall preclude a covered utility from using customer aggregate data for analysis, reporting, or program management if all information has been removed regarding the individual identity of a customer.