DOCKET NO. E-100, SUB 161
BEFORE THE NORTH CAROLINA UTILITIES COMMISSION

In the Matter of:	)	
Commission Rules Related	)	REPLY COMMENTS
To Customer Billing Data	)	OF MISSION:DATA COALITION
	)	

REPLY COMMENTS

Pursuant to the North Carolina Utilities Commission's (the "Commission") May 26, 2020, Order Requesting Reply Comments, and the Commission's Rules of Practice and Procedure, the Mission:data Coalition ("Mission:data") hereby files the following reply comments on the proposed data privacy and data access rules in the above-captioned docket.

As discussed below, Mission:data and the North Carolina Attorney General's Office ("AGO") submitted a jointly-developed proposed data portability and data privacy rule (revised R8-51) with their initial comments. That draft rule represents the state-of-the-art reasoning and strikes the appropriate balance between data access and the substantial benefits flowing from such access, and legitimate privacy concerns at the utility and customer level. Since submitting the revise R8-51, Mission:data has reconsidered certain sections of the proposed rule and concluded that several changes are warranted to clarify the draft language. Attachment A to these reply comments is a "redlined" version of the draft rule showing the modifications needed to clarify the intent.

1. BACKGROUND

The present docket was opened in February, 2019 upon the recommendation of the Public Staff for a rulemaking aimed at promulgating rules governing access to customer energy usage and billing data held by a utility, while at the same time protecting utility information systems and customer privacy. On February 10, 2020, the Public Staff filed initial comments and proposed amendments to Commission Rules R8-7, R8-8 and R8-51. On the same day, Mission:data and the North Carolina Attorney General's Office ("AGO") filed separate comments but also included with their comments a jointly-developed proposed data portability and data privacy rule for the Commission's consideration (revised R8-51). The Public Staff and Mission:data/AGO were the only parties to submit draft proposed rules. Other parties also filed comments on February 10, 2020; however, these comments primarily critiqued the Public Staff's proposed rules which had been circulated among the parties prior to the close of the initial comment period. Below, the Joint Parties respond to the initial comments filed by Duke Energy Progress, LLC and Duke Energy Carolinas, LLC ("Duke"), Virginia Electric and Power Company d/b/a Dominion Energy North Carolina ("Dominion"), the Public Staff, and the City of Asheville ("Asheville").

As noted above, the Public Staff's proposed rules were circulated among the interested parties before the initial comment period ended and, in effect, represented "trial rules" for the interested parties to assess. These reply comments will now provide the Public Staff an opportunity to respond to the comments on its proposed rules. The same, however, cannot be said for the proposed rule proffered by Mission:data and the AGO. The initial comments were the first time the Mission:data/AGO proposed rule was presented to other interested parties in a comprehensive way. These reply comments will be the first opportunity for the parties to formally comment on that proposed rule and, as it now stands, Mission:data and the AGO will not have the opportunity to

formally respond to those comments. Mission:data believes it is important for the Commission to allow sur-reply comments thereby permitting Mission:data, the AGO and any other party so inclined to address the issues raised in these reply comments regarding the Mission:data/AGO proposed rule. The topics in this docket are complex. They involve first-party and third-party access to customer data, the latter with customer permission, and privacy. Each of these issues presents a variety of technical and legal dimensions. Mission:data believes the record will be significantly enhanced by allowing a thorough vetting and analysis of the topics as delineated in the Mission:data/AGO proposed rule. We therefore respectfully request that the Commission grant leave for all parties to file sur-reply comments.

A. COMMISSION RULES SHOULD MAXIMIZE THE BENEFITS TO CONSUMERS OF SMART GRID INVESTMENTS BY ENABLING THIRD PARTY INNOVATORS TO ACCESS CUSTOMER ENERGY DATA WITH CUSTOMER PERMISSION

Mission:data's primary objective in this rulemaking is to ensure that the rules ultimately adopted deliver maximum value to consumers, while protecting data privacy. Maximum value will be achieved (a) by creating a platform where consumers benefit directly from the substantial investments the utilities have made and continue to make in advanced metering infrastructure ("AMI"); and (b) by providing consumers the ability to capitalize upon new, innovative energy-saving services that utilize the data generated by AMI to identify, analyze and capture substantial energy savings. Most of these new innovative energy-savings services are provided by third parties and otherwise are not available from the regulated utilities. Distributed energy resources ("DER") supplied by third parties can help customers cost-effectively manage their energy bills, whether through rooftop solar, tailored energy efficiency smartphone "apps," building energy optimization software, or similar innovative technologies. These energy saving innovations are occurring nationwide, but for the most part, are available only from non-utility providers. Mission:data strongly

believe that consumers should be allowed to directly benefit from the innovations that are now possible as a result of the utilities' investments in AMI.

Furthermore, Mission:data strongly believes that the benefits now possible can be realized without jeopardizing privacy. In fact, in recent years five (5) state public utility commissions have mandated data privacy and data portability rules, meaning that customers can opt to have their utility share their energy-related information (including usage, billing and account information) directly with a third party via secure, standardized electronic transmission. These five states – California, Colorado, Illinois, Texas and New York – have 36.2 million smart electric meters, representing 37% of the nation's 98 million smart meters deployed as of December, 2019.[1] Breaches in privacy have not been a problem; substantial cost-effective energy savings, however, have been realized.

B. THE THEORY THAT CONSUMERS WILL BENEFIT JUST AS MUCH FROM THE ABILITY TO ACCESS DATA ON UTILITY WEB PORTALS IS UNREALISTIC AND NOT SUPPORTED BY ACTUAL EXPERIENCE.

At the outset, it is important to understand and emphasize the *critical distinction between competing theories* held by the parties in this docket about *how* customers are most likely to benefit best from the ability to access energy usage and billing data now available with the emergence of AMI. As is evident from their comments, the utilities tend to point to their customer web portals to argue that access to the raw energy usage and billing data available on these portals is all that is needed to educate consumers, promote consumer change and satisfy public policy objectives. The utilities' theory is based on the somewhat unrealistic notion that consumers will systematically visit the web portals, download their data, analyze it and then make the appropriate lifestyle changes and purchases to foster energy savings and economically optimal outcomes.

1 Edison Foundation Institute for Electric Innovation. *Electric Company Smart Meter Deployments: Foundation for a Smart Grid (2019 Update)*. December, 2019 at 1. Available at https://www.edisonfoundation.net/-/media/Files/IEI/publications/IEI_Smart-Meter-Report_2019_FINAL.ashx.

Mission:data submits that this theory is fundamentally flawed and quixotic. Indeed, the evidence shows that consumers are unlikely to maximize efficiency benefits by themselves from utility web portals. Third party involvement via real-time analysis of usage data and billing information is essential to serve those customers who desire to manage their energy more efficiently. This view point is underscored by the fact that *utility web portals from across the country have low utilization rates* – particularly the portions of utility web portals devoted to displaying energy usage – and the availability of such web portals has, to our knowledge, led to negligible reductions in energy usage. Moreover, the point is further underscored in a report by the Department of Energy about AMI which concludes that "[m]any utilities deploying smart meters with web portals have experienced difficulties attracting customers to access and use their web portals, and the ultimate value of these tools is still an open question."[2]

The limited effectiveness of web portals alone is also demonstrated by the reality of consumer marketing and behavior trends: consumers purchase new products and services after hearing about them from friends and family, seeing advertisements on social media, or searching online. DER products and services are no different. If a customer is interested in a smartphone "app" for managing household energy use over time, it is unlikely that they will be attracted to one where they are required to go to their utility's website, once per day, to download information and then upload that information to their app. Instead, that customer is much more likely to begin managing their energy usage when they can authorize electronic data-sharing, and begin using the energy management app with minimum friction – just like how consumers use Paypal for authorizing payments, Facebook for logging in and commenting on websites, Google for connecting voice

2 U.S. Department of Energy. Smart Grid Investment Grant Program. *Customer Participation in the Smart Grid - Lessons Learned*. September 2014, at 14. Web: http://energy.gov/sites/prod/files/2014/10/f18/SG-CustParticipation-Sept2014.pdf

assistants with in-home devices, or budgeting software for accessing their financial records at different financial institutions. Today's consumers expect interactions with their service providers to be seamless and digital – particularly when two service providers need to interact with one another.

This theory of consumer behavior is not only more realistic but it is necessary to meet modern consumers' digital expectations now and into the future, and it is necessary to conform with industry best practices. For these reasons, Mission:data endorses the Public Staff's recommendation that utilities be required to implement Green Button Connect ("GBC") by January 1, 2022. *See, Initial Comments and Proposed Draft Rules of the Public Staff*. Docket No. E-100, Sub 161 (February 10, 2020) Proposed Rule R8-51 subsections (d), (g) and (h). GBC enables the standardized, streamlined, electronic transmission of energy data to customer-authorized DER providers. In this manner GBC meets consumer expectations, maximizes customer use of AMI data and increases the efficacy of energy savings programs. Mission:data wholeheartedly agrees with the Public Staff that the data portability and privacy rules developed in this docket should allow "customers [to] realize the full benefits of smart meters and robust customer information systems of the utilities."[3]

With that said, however, the Joint Parties believe the Public Staff's proposed amendments fall short of maximizing benefits for customers in several respects. Below, we reply to Public Staff's proposed rules, as well as reply to the initial comments of Duke, Dominion, and the City of Asheville.

2. REPLY TO DUKE

A. Duke Argues Inconsistently That GBC Requires Resource-Intensive Technical Review, Whereas Other Modifications Proposed by The Public Staff Do Not

The Public Staff proposes numerous changes to Rule R8-51 that would impact Duke's business systems, process, and Customer Connect platform. In response, Duke states that it is

3 Initial Comments and Proposed Draft Rules of the Public Staff. Docket No. E-100, Sub 161 (February 10, 2020) at 3.

"generally supportive of the Public Staff's proposed Rule R8-51."[4] Indeed, with respect to virtual all of the changes outlined in the Public Staff's proposed Rule R8-51, Duke essentially suggests that it will be able to assimilate the requirements without the need for multiple years to research to evaluate and design a solution, establish business and administrative processes, and address cybersecurity topics. Duke also nowhere suggests that the costs of complying with these proposed system and design changes will be unreasonable or disproportionate to the benefits. Yet, this positive inclination towards the Public Staff's proposed rule all changes when it comes to the proposal to make GBC mandatory beginning January 1, 2022 (proposed R8-51 subsections (d), (g) and (h)). That proposal would require analogous changes. Yet, with respect to those analogous changes, Duke objects on the basis of cost, requisite operational and design modifications, cybersecurity and other grounds. This inconsistent attitude toward comparable proposed changes is worthy of the Commission's close scrutiny because it indicates a clear double standard.

The Public Staff's proposed Rule R8-51 would, if adopted, cause several key modifications to the utilities' business processes and customer information systems. For example, in the revised R8-51, the Public Staff proposes that utilities: (i) provide aggregated energy data to customers or authorized third parties subject to passing certain mathematical tests; (ii) maintain customer data in "electronic machine-readable format that conforms to nationally-recognized standards and best practices"; and (iii) provide "the ability and means [for customers] to terminate ongoing consent" for information shared with a third party. Although these changes would require modifications to a utility's systems and processes, Duke states that it understands and "generally supports" the proposal.

This all changes when it comes to GBC, a proposal that would *similarly* implicate Duke's customer information systems and business processes. Here, Duke argues that it does not

---

4 Initial Comments of Duke Energy Carolinas, LLC and Duke Energy Progress, LLC. Docket No. E-100, Sub 161. Filed February 10, 2020 at 3.

"understand" the requirements and needs significant time and resources to thoroughly evaluate – let alone implement – the change. In response to an informal information request asking Duke to explain its concern and in particular the statement in its initial comments that GBC would "add risk" to the deployment of Customer Connect, Duke stated:

> Additionally, the Companies believe numerous details must be considered before implementing the functionality described in the paragraphs (d), (g) and (h) of the proposed [Public Staff] Rule [that would require GBC by January 1, 2022]. For example, if this process is to be fully automated, questions regarding customer privacy, including tracking and understanding customer consent, as well as the costs for tracking and understanding customer consent, would need to be determined, quantified, and designed. **Furthermore, the requirements to support this capability are unknown, and the Companies believe a project would be needed to assess the level of effort and cost to implement this functionality**. As noted above, the design and build of Customer Connect is nearly complete, and testing of the solution has begun; therefore, any project to assess the requirements to implement [GBC] could not begin until 2023, after the deployment and stabilization of Customer Connect.

Duke's differential responses to comparable proposed requirements in the Public Staff's proposed rule are inconsistent and contradictory on their face. Essentially, Duke is saying that with the exception of the proposed requirement to adopt GBC by January 2022, the impact of the Public Staff's proposed changes to R8-51 on systems and designs, including the Customer Connect platform, have been thoroughly evaluated and are not problematic; however, the impact of the requirement to adopt GBC has not been looked at and could not begin to be evaluated until after 2023 when the Customer Connect program has been fully deployed and stabilized. With all of the sensitivity and risk that Duke claims is associated with delivery of Customer Connect, it simply is difficult to believe that one set of modifications to Customer Connect that will result from the

Public Staff's proposed revisions to R8-51 has been thoroughly vetted, designed, and quantified by Duke, whereas another has not.

B. Duke's Argument Would Hold Any Commission Rulemaking Hostage to Duke's Information Technology Systems

Another argument Duke puts forth in opposition to GBC is that modifications to its Customer Connect platform cannot be implemented until 2022 or 2023. Duke states: "Implementation of these proposed Rule amendments [adding GBC] in January 2022 will add risk to the deployment of the Customer Connect Program for DEC (April 2021) and DEP (April 2022)."[5] Furthermore, not only does Duke argue that *implementation* of GBC would imperil Customer Connect, it also argues that merely *evaluating* GBC before 2022 or 2023 would similarly put the delivery of Customer Connect at risk.

Duke's argument would force proposed regulations designed to promote energy-efficiency and energy savings, and all of the attendant benefits like carbon reduction, to *accommodate the utility and its schedule*, rather than requiring *the utility to accommodate the regulations and the public policies underlying those regulations*. Accepting Duke's premise would result in a functional "carve out" or freeze on public-interest regulation; that is, anything that would affect Duke's customer information systems would have to be delayed or held in abeyance for several years. For example, what if a new threat to online privacy developed in 2021? Would Duke claim that it could not evaluate or implement any changes to address the threat until after 2023 when Customer Connect had been appropriately "stabilized"? The Commission should roundly reject any argument that makes public utility regulation subservient to information technology.

---

5 *Id.* at 4-5.

C. Duke's Existing Processes for Third Party Data Requests Are Inadequate and Fall Short of Best Practices in The Utility Industry

In addition to the above arguments against GBC, Duke also states that "the Companies [DEC and DEP] already have a process to field third-party data requests for customer usage data and billing information."[6] The clear implication underlying this claim is Duke's conviction that GBC is unnecessary and duplicative. Duke's existing process for handling third party data requests, however, is inefficient, arduous, expensive and out of step with best practices in the utility industry. It is not a proxy or a substitute for GBC.

First of all, Duke's process for handling data requests is *manual*. And, while a manual process may be appropriate for "one-off" requests of monthly usage and monthly billing data, it is extremely ill-suited for today's landscape where customers with advanced meters seek to capitalize on a constant flow of data and information and the technologies that turn that flow into real energy savings. A manual system will become even more antiquated with time as AMI becomes more prevalent and DER services using innovative technologies to enhance energy efficiency and bill savings continue to penetrate the market. A continual flow of data and information to customer-authorized third parties is essential for any customer to realizing value from AMI investments and emerging technologies. A manual system cannot meet this demand.

Second, Duke's existing process for handling third party data requests is cumbersome and expensive, and produces comparatively stale data. Today, if a Duke customer wants Duke to transmit its usage, billing or account information to a third-party service provider, the customer embarks on a multi-step, time-consuming, costly process. First, the customer tells the third party to print, complete and sign an "Energy Data Request Form." The third party scans the form and submits it by email to BSCTeam@duke-energy.com. After several business days of processing, the third party receives an

6 *Id.* at 5.

automated reply form requesting the customer to complete another a "Customer Data Release Form." Then, the third party is sent a bill for $48 per request, plus a variable fee of $0.20 per customer requested. Once payment is received, the information is sent to the third party via secure email within 10 business days.[7]

The most obvious shortcoming of this process is that it is wholly unworkable for a third party to receive customer energy usage data on an *ongoing* basis to help the customer manage their utility bills and provide recommendations for energy efficiency improvements. Modern software applications for energy management involve *continuous* monitoring of trends in order to spot waste and notify the customer so that he or she can take action. For example, residential customers in several states can retain a third party that sends weekly emails analyzing their usage patterns, providing a breakdown or "disaggregation" of where electricity was consumed in the home, and suggesting how to reduce plug loads such as electronics that remain turned on 24 hours a day. Energy savings and bill savings in these circumstances have amounted to 6% to 18% or more, a substantial economic benefit to consumers.[8] Using Duke's existing process, however, the software provider would need to submit weekly requests to Duke, thereby incurring a bill of $2,496 in a single year ($48 * 52 weeks/year), an amount that exceeds many North Carolina ratepayers' electricity bills over the course of one year and derailing any possible savings.

For commercial customers, another example of a software offering involves weekly emails compiling and analyzing daily data and making recommendations for managing energy use and reducing peak demand. The service includes a web portal so that the building operator can make a change in heating and cooling systems and see that quickly reflected in energy usage trends. In order

7 See *Duke Energy Progress response to Data Request No. 1 of Environmental Defense Fund* in Docket No. E-2 Sub 1142, dated October 11, 2017.

8 *Got Data? The Value of Energy Data Access to Consumers*. Mission:data Coalition. January, 2016. Available at http://www.missiondata.io/s/Got-Data-value-of-energy-data-access-to-consumers.pdf.

to provide this daily analysis of energy usage data for commercial building customers, the customer or the third party would, under Duke's present system, incur a bill of at least $17,520 (paying $48 for 365 days per year). In addition, since data requests are processed in Duke's existing system after 10 or more business days, it would be impossible to promptly notify a commercial building operator of a malfunction (*e.g.*, malfunctioning compressor) that should be repaired immediately. Instead, the building operator would receive the notification almost two weeks after the malfunction occurred.

The time, cost, manual back-and-forth of consent forms, and delay in receiving information and data, deprive customers of the energy efficiency benefits that AMI promised to provide. The inefficiency of Duke's existing processes is reflected both in the $48 charge as well as by the fact that numerous other investor-owned utilities across the nation have implemented GBC, making streamlined, continuous and automated energy information available at no cost to either consumers or third parties. As mentioned previously, utilities in five (5) states, representing over 36 million electric meters nationwide, are mandated to provide GBC as part of basic utility service. While Duke proceeds with its massive Customer Connect project – an investment of some $900 million across all Duke operating companies – Customer Connect will *be significantly outdated* on "day one" because it does not provide electronic data portability like many of Duke's peers.

D. Green Button Connect Is Consistent with Duke's Corporate Strategy, Press Releases and Sworn Testimony

It is important to underscore that, contrary to Duke's arguments in its initial comments, GBC is, in fact, entirely consistent with Duke's corporate strategy as stated in various documents including press releases, and the sworn testimony of its executives with regard to smart grid and advanced metering. For several years, Duke operating companies have praised the ability of the "smart grid" to support an ecosystem of customer applications that manage customer energy usage. GBC would

fulfill those objectives in a manner consistent with open standards and an open architecture. Below are representative statements from Duke demonstrating that GBC is consistent with Duke's corporate objectives:

- "SmartGrid, however, is not limited to AMI metering. The possibilities with SmartGrid technologies are infinite as it is continuously evolving much like the internet has evolved over time. SmartGrid is much more than simply the functions it is capable of performing. It is an open architecture integration of the electric distribution system which will provide capabilities and/or a platform for emerging technologies."[9]

- "We believe SmartGrid will be the foundation for technology that is being developed that will enable customers to have more granular information at the device or appliance level."[10]

- "Duke Energy is leading the industry's digital grid transformation by assessing, developing and implementing an end-to-end digital grid system that lays the groundwork for an energy evolution where information and automation will enable customers and companies to work together to keep energy affordable, reliable and clean."[11]

- "Think of the communications node as an iPhone® for the modern grid. It is a device with the future communications capability for multiple networks, with capability to route the data between multiple devices and with enough storage and processing power to enable an extensible ecosystem of data applications which are anticipated to be built over a number of years."[12]

- "Duke Energy is an active participant in the National Institute of Standards and Technology (NIST) standards development process and contributes thought leadership on national standards. Duke Energy actively works with several standards bodies and trade organizations to ensure that we can obtain the proper alignment with the standards as they are adopted."[13]

---

9 *Direct Testimony of Todd W. Arnold on Behalf of Duke Energy Ohio*. Public Utilities Commission of Ohio, Case Nos. 08-920-EL-SSO, 08-921-EL-AAM, 0899-EL-UNC, 08-923-EL-ATA. July 31, 2008 at 3:11-16.

10 *Id.* at 11:4-6.

11 *Duke Energy: Developing the communications platform to enable a more intelligent grid*. David Masters, Manager, Technology Development at Duke Energy. February 1, 2011 at 4.

12 *Id.* at 7.

13 *Id.* at 15.

- "Duke Energy will continue to innovate and collaborate with its ecosystem of partners to identify, develop, and incorporate new applications and technologies that best leverage this platform for the digital grid."[14]

One can only conclude that Duke's opposition to GBC now in this docket is selective. Duke claims to support National Institute of Standards and Technology (NIST) standards; NIST developed GBC, which Duke opposes here. Duke also states its philosophy is to "incorporate new applications and technologies" that make use of the "digital grid," and yet in this docket Duke opposes one of the best-known standards available for consumers to access innovative software applications. If a smartphone app maker wants to help consumers manage their monthly bills, Duke apparently is unwilling to make modest changes to its IT systems to meet modern customers' expectations. But, at the same time, Duke has sought and won billions of dollars of ratepayer funds for technology investments that are closed and can only be utilized by Duke. It would appear that Duke supports national standards and interoperability selectively; that is, if Duke perceives a threat to its monopoly control over information about electricity usage, then its commitment to standards evaporates.

Finally, adherence to nationally-adopted standards is critical for the smart grid to reach its full potential. Conforming with technical standards such as GBC ensures that ratepayers have access to the full range of DER products and services that are developed nationwide. Consistent interfaces mean that, for example, a smartphone "app" developed in Colorado or Virginia for managing energy usage could be used by customers in North Carolina. The greater the deviation from standards, the more expensive it is for third party DERs to operate in a given jurisdiction. Thus, while Mission:data applauds Duke for its stated commitment to national standards, it is important to note that Duke has not always been willing to adopt them. For example, during a

14 Id. at 16.

rate case hearing, when DEC was pressed on its adherence to the Green Button Download My Data standard, DEC equivocated:

> Q. And then just moving on to another topic. Dr. Weintraub, you mentioned that one of the offerings that the Company is providing is Green Button Download My Data. That will be available at the end of this year?
> A. (Weintraub) What we will be offering is the functionality associated with being able to download your data.
> Q. Okay. And what does that mean, "the functionality"? You're offering that functionality, but you have not adopted the actual Green Button standard?
> A. That's correct.[15]

Similarly, in another case in Kentucky, Duke Energy Kentucky stated that "Duke Energy Kentucky is not proposing to implement the Green Button Standard because the Duke Energy portal and associated programs will provide the same functionality and greater flexibility for customers."[16] The details of such functionality and "flexibility" were not explained or provided.

All of this is to say that Duke's adherence to national standards, particularly with regard to customer data access topics, should not be assumed. The Commission should be diligent in requiring that information technology systems be built according to the GBC standard. For Duke to truly embrace national standards, it should not object to GBC or to Section (e)(2) of the Mission:data/AGO proposed rule, which requires adherence to the latest version of the North American Energy Standards Board's ("NAESB") GBC standard.

15 Evidentiary hearing in Docket No. E-7, Sub 1146, *In the Matter of Duke Energy Carolinas, LLC for Adjustment of Rates and Charges Applicable to Electric Utility Service in North Carolina*. February 26, 2019. Transcript at 113:9-20.

16 Kentucky Public Service Commission Case No. 2016-00152. Attorney General's Second Set Data Requests (AG-DR-02-013). Date received: June 20, 2016 at 2. Available at https://psc.ky.gov/pscecf/2016-00152/debbie.gates%40duke-energy.com/07052016014910/Case_No._2016-00152.pdf.

E. Duke's Cybersecurity Concerns About GBC Are Misplaced

Duke appears to be concerned that GBC introduces cybersecurity risks that it would not otherwise face. In initial comments, Duke states:

> The potential risks of third-party involvement in that process should be fully vetted before a Commission Rule requires it, even if the requirement begins in 23 months. Third-party access could require a stringent approval process with significant security requirements, leading to potential resource challenges as requests line up in a queue for data.[17]

Here, it is extremely important to distinguish between "system risks" and "third party data misuse risks." System risk is the cybersecurity threat utilities face by having *any* non-utility entity access their IT systems; data misuse risk is the risk that a customer-authorized third party will abuse the customer's privacy rights after receiving information from the utility. This distinction is important because under a well-defined data portability and privacy rule the utilities, like Duke, are responsible only for their *own* system risks, not data misuse risks stemming from a customer-authorized third party. Thus, cybersecurity risks within the sphere of the utilities' responsibility – system risks -- are well-defined and are generally limited to risks the utilities should be addressing in any event.

This paradigm is reflected in the Mission:data/AGO proposed rule. Section (g) states: "Nothing in this Rule shall be construed to impose any liability on a utility….relating to disclosures of information when...a customer discloses covered data to, or authorizes access to standard customer data by, a third party that is unaffiliated with and has no other business relationship with the utility." Section (d)(4)(ii) makes a utility responsible only for its acts and those of a utility contractor or vendor that accesses the utility's IT systems. The Mission:data/AGO rule makes clear that utilities

17 Initial Comments of Duke at 5-6.

are *not* responsible for the acts of a customer-authorized third party, whom the utility does not control, but is responsible only for maintaining reasonable security practices on its *own* IT systems.

According to Duke, GBC presents potentially hazardous cybersecurity risks that would require "a stringent approval process" of customer-authorized third parties. Again, under the Mission:data/AGO rule utilities are not responsible for third-party data misuse. That risk lies with the customer retaining the third-party service provider. The utilities are responsible only for system risk. The Mission:data/AGO rule clearly and comprehensively defines these concerns and requires only that the utilities adopt reasonable cybersecurity protections on their *own* IT systems, such as, restrictions on using customer data solely for the purpose of providing regulated utility service (Section (d)(1)); requirements that contractors to the utility maintain "policies, practices and notification requirements no less protective than those under which the utility itself operates" (Section (d)(4)(ii)); requirements that utilities implement "reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use modification, or disclosure" (Section (p)(1)); and annual data privacy and security audits (Section (t)). These are highly tailored requirements and represent good operating practices. In all likelihood they are already part of the utilities' cybersecurity program and efforts to confront system risks.

Finally, contrary to Duke's assertions, any GBC platform can and should be "unhackable." It is the utility's responsibility to ensure that its systems are protected. If a utility's GBC platform is breached by anyone, it means the utility has acted negligently. The GBC technical standard ensures that *customer data is only released with customer consent*, and that such release occurs via Transport Layer Security, *i.e.*, an encrypted channel. If the GBC platform is successfully attacked, that can only be because the utility has not adequately prepared and managed its systems. In contrast, it should be noted that utility web portals are accessible to the public internet and face similar risks of intrusion by

unknown entities – but Duke does not argue that its web portal should be shut down due to these cybersecurity risks. In contrast, the GBC platforms are not exposed to the public internet, which significantly reduces their risk profile as compared to web portals.

As for *data misuse* risks, the Commission should explicitly waive utility liability so long as customer data is transferred pursuant to customer consent and is encrypted in transit. *See,* Section (g) of the Mission:data/AGO rule. A tailored liability waiver of this kind is both necessary and appropriate because, without it, the utilities will necessarily take on a "policeman"-type role over customer-retained DERs that utilize GBC. Duke's anxiety about policing customer-authorized third parties is therefore unfounded under the Mission:data/AGO rule. While it is reasonable and necessary for utilities to "police" the data management practices of their vendors, the same is not true of DERs that utilize GBC with customer consent.

F. Duke's Stated Concerns About GBC Cybersecurity Are Contradicted by Duke's Existing Methods of Information Exchange with Third Parties

As mentioned above, Duke alludes to cybersecurity concerns associated with GBC, arguing that "[t]he potential risks of third-party involvement in that process should be fully vetted before a Commission Rule requires it [GBC]…" This concern for "thorough vetting" in the case of GBC, however, is somewhat belied by how Duke currently exchanges customer account and billing information with certain commercial customers and their authorized third parties. In those cases, no hyper "vetting" or enhanced cybersecurity qualifications are required by Duke, a letter of authorization is all that is required. This is indeed curious and again suggests a double standard. Duke's opposition to GBC seems to be little more than a selective dislike rather than an objective, fact-based assessment.

In response to an informal information request, Duke explained that it uses electronic data interchange ("EDI"), which is an older method of transmitting certain customer data over File

Transfer Protocol ("FTP")[18] with certain commercial customers, particularly those with many dozens or hundreds of locations, and their authorized third parties. When asked to provide further information about the *contractual requirements* Duke imposes on the third parties accessing customer data with permission of the customer, Duke stated there are none:

> With Customer Connect, we will use a third-party vendor to provide the EDI Billing Information to trading partners. We will transmit the data to our vendor using Secure File Transfer Protocol (SFTP) and Pretty Good Privacy (PGP) encryption, ensuring it is secure and encrypted both in transit and at rest. The vendor sends the EDI Billing information (EDI 810) primarily using a value-added network (VAN); there are some trading partners that utilize a direct connect with SFTP. EDI trading partners must have a way to interpret the EDI data, typically using specific software obtained by the trading partner. **If the trading partner is not the customer of record, Duke Energy requires a letter of authorization (LOA) before the EDI billing information is provided to the third party. There are no other contractual requirements** (emphasis added).

Thus, once again, it appears that Duke's claims of cybersecurity threats are selective. EDI has been used for many years and by using it, Duke exchanges sensitive, personally-identifiable account and billing records *with third parties for whom there are no privacy or security requirements*. The only prerequisite to the use of EDI is a *letter of authorization* from the customer. GBC, like the EDI system Duke describes above, also requires customer authorization prior to exchanging data. Why more would be required in the case of GBC is not clear. If customer-authorization is all that is necessary in the case of information exchanged by EDI, it is not clear why customer authorization would not satisfy Duke's requirements for GBC. Put another way, the Commission should dismiss Duke's argument that GBC introduces novel risks. Duke's existing EDI process shows that its opposition to GBC based on cybersecurity is selective and not based on objective fact.

18 EDI originated in the 1970s for electronically exchanging purchase orders and invoices between military contractors. Utilities often use EDI today for exchanging customer data with retail suppliers in states with competitive retail electric markets. See https://en.wikipedia.org/wiki/Electronic_data_interchange.

3. **REPLY TO DOMINION**

Dominion adheres to the theory that optimal energy-savings can be realized from a customers' ability to access their own data on Dominion's web portal. As noted above, customer access to raw data on a web portal is unlikely to result in optimal energy-savings; the evidence shows that more is required. Nevertheless, with this fanciful theory in mind, Dominion praises the Public Staff's draft rule because it "aligns with the Company's goals to ensure customers can access, use, and understand their own data in a secure manner."[19] Beyond this limited endorsement, Dominion objects to the data portability provisions in Public Staff's proposal that would come into force January 1, 2022 – Green Button Connect or GBC.

Dominion's first objection to GBC is that "it is premature to prospectively adopt by reference a standard nearly two years in advance that could change substantially before it is automatically codified into the Commission's rules."[20] This objection is misplaced for two reasons.

First, Dominion is already obligated to abide by numerous standards that could "change substantially" over time. For example, Internet security standards implicating Dominion's web portal such as transit-layer encryption and intrusion detection systems are constantly changing, as are various NIST critical infrastructure protections. Dominion does not appear to object to adhering to those standards today even though those standards undoubtedly will evolve over time. Furthermore, it is not uncommon for a rule or regulation to go into effect while providing a lead-time to implement the program or provisions required by the rule. In fact, this is quite common and to object on the basis that conditions or circumstances might change at some time in the future is to provide no basis for the objection at all.

19 Initial Comments of Dominion at 3.
20 Id. at 15.

Second, contrary to Dominion's concern with potential "substantial changes" before implementation of GBC is required, the reality is that the Energy Services Provider Interface ("ESPI") standard, the standard initiating GBC, has not changed significantly since being adopted.[21] For example, the last update by the North American Energy Standards Board ("NAESB") in April 2019, formally adopted a format change for certain customer information such as premise addresses and monthly bills. The change was a formality and not substantive in nature. And, contrary to Dominion's concern, it was already in use by multiple utilities for several years prior to its formal adoption. The April 2019, update made no material changes to the data format for energy usage data, which has been in place and stable since 2013. To put it another way, implementers of GBC know that some changes do occur over time, but those changes are modest and no different from periodic updates that occur with any software system.

Dominion's second objection to GBC is that it would "require" Dominion to impose cybersecurity requirements on third party recipients of customer data. Dominion states that Public Staff's proposal "does not address the ability of utilities to properly vet prospective connecting third parties and the associated risks to the utilities' network security."[22] This issue has been discussed in some detail above in response to Duke's similar concerns. *See,* Section 3.E., pgs. 16 to 18, above.

Moreover, while the Public Staff's rule does not address issues such as qualifications for customer-authorized third parties, the Mission:data/AGO rule does. In Section (f)(9) of the Mission:data/AGO rule set forth specific eligibility criteria for customer-authorized third parties including that they must 1) demonstrate technical capability to interact securely with the utility's

[21] The ESPI standard was adopted to provide an accepted process and interface for the exchange of retail customer energy usage data and to support the development of innovate products that allow consumers to better understand their energy usage and make more economical decisions related to their energy consumption. It is the foundational standard for GBC.

22 Id. at 16.

servers; (2) provide contact information and federal tax identification numbers to the utility; (3) acknowledge receipt and review of these privacy and access rules; (4) not have been disqualified as an authorized third-party provider in the past pursuant to processes outlined at Section (h)(2)-(4) of the Mission:data/AGO proposed rule; and (5) adopt and comply with the most updated version of the Department of Energy's Voluntary Code of Conduct Final Concepts and Principles for Data Privacy and the Smart Grid ("DataGuard"). Notably, DataGuard requires that third parties have a cybersecurity risk management program, which includes, among other requirements, an assessment of risks, reasonable technologies and processes for protecting against loss and unauthorized use of data, and a comprehensive data breach response program.[23] Thus, Dominion's concerns regarding qualifications for customer-authorized third parties is adequately addressed and reconciled in the Mission:data/AGO proposed rule.

Like Duke, Dominion does not distinguish between "system risks" and the risk of data misuse by customer-authorized third parties. The Mission:data/AGO rule not only acknowledges that distinction but also clearly delineates lines of responsibility, limiting the utilities' responsibility to maintaining the cybersecurity of its *own* systems only. The Mission:data/AGO proposed rules also establish eligibility criteria for third parties; delineate the circumstances under which a utility is not liable for a customer-authorized third party's data misuse; and, in Section (h)(3), outline a process by which a utility's reasonable suspicion of a third party's breach of privacy rules can be reported to the Commission. Plainly, the Mission:data/AGO rule thoroughly address all of the concerns relating to GBC that are raised by Dominion and if Dominion faults the Public Staff's proposed rule for lacking

23 DataGuard Voluntary Code of Conduct Final Concepts and Principles. Available at https://www.dataguardprivacyprogram.org/downloads/DataGuard_VCC_Concepts_and_Principles_2015_01_08_FINAL.pdf

these elements, the simple answer is not to jettison a beneficial program entirely, but rather, to adopt the Mission:data/AGO proposed rule or the relevant portions thereof.

4. REPLY TO PUBLIC STAFF

As mentioned above, Mission:data supports the Public Staff's requirement to implement GBC by January 1, 2022. With that said, there are three issues in the Public Staff's proposed rule, ranging from cost recovery to utility liability, that should be addressed.

First, the Public Staff proposes that utilities be permitted to charge third parties a Commission-approved fee to access customer data. Proposed section R8-51(e) of the Public Staff's proposed rule states:

> Other authorized third parties may be charged Commission-approved fees for customer data. All parties, including customers, may be charged Commission-approved fees for aggregated data. The fees charged for customer data must be commensurate with the costs the utility incurs in assembling, compiling, preparing, and furnishing the requested customer data.

However, once GBC is implemented by January 1, 2022, the marginal cost to "assemble, compile, prepare, and furnish the requested customer data" will be zero. As with software in general, the software for GBC has an up-front cost to deploy, but zero marginal cost to operate.[24] It seems the particular provisions in proposed R8-51(e) were written for pre-existing manual processes and not modern, electronic ones.

In addition, cost recovery for a zero-marginal-cost service such as GBC can be extremely complex. With zero marginal costs the only costs incurred are the fixed costs. An equitable allocation of these costs will require knowledge of the number of transactions over the life time of the

24 Of course, costs are incurred for maintaining information technology systems in terms of security and functionality upgrades. However, our point is that, in an automated software system, the incremental cost of a customer request to share his or her data is zero.

system. This figure effectively is an unknown as there no way to accurately predict the number of customers that will utilize GBC during its operating life. Given this uncertainty, and the fact that customers should not have to pay an additional fee to take advantage of rate-based assets such as advanced meters that were installed ostensibly to benefit them to begin with, substantiates that no fees should be imposed for "standard" customer data via GBC.

Second, the consent form described in Public Staff's proposed rules does not adequately accommodate the realities of modern, electronic, web-based authorizations that are commonly used on the internet today. Public Staff proposes that a consent form – even one available electronically – must include third party mailing addresses and telephone numbers. This goes against modern standards and will confuse customers who wish to share their information with a software company. Customers are familiar with online processes that identify a company to which a customer's data will be shared, but never do such web-based forms provide a physical address or telephone number. For example, who knows what Facebook's telephone number is? Billions of dollars per month are transferred via Paypal using online transactions that do not require the customer to know Paypal's mailing address and telephone number. The point is that transactions of the utmost sensitivity – including sending large amounts of money all over the world – occur routinely without antiquated forms. The Mission:data/AGO rule would require that the authorized third party provide its complete contact information to the utility, but it deliberately does *not* require that *customers* provide contact information on the consent form, because it is unnecessary and burdensome for customers. Unlike Public Staff's draft Rule R8-51(e), the Mission:data/AGO rule is consistent with modern online services in this respect.

Third, there are numerous subtleties not captured in Public Staff's proposed Rule R8-51 that *are* described in detail in the Mission:data/AGO rule. Important details, such as the fact that a utility

should encrypt customer data while in transit to a third party, are comprehensively included in the Mission:data/AGO rule but left out of the Public Staff's proposal. As a result, the Mission:data/AGO rule is superior and should serve as the basis for discussion going forward in this docket.

5. **REPLY TO CITY OF ASHEVILLE, WHO ADDRESSES THE IMPORTANCE OF BILLING AND ACCOUNT INFORMATION, IN ADDITION TO ENERGY USAGE DATA**

In its comments, the City of Asheville ("Asheville") supports three (3) general concepts related to data access, and recommends specific changes to three (3) sections of Public Staff's draft rule. Asheville's stated position and concerns are legitimate and are addressed in the Mission:data/AGO proposed rule.

Asheville argues for three outcomes to support the city's energy efficiency and carbon reduction efforts: (i) aggregated energy data should be available to the city, including data on efficiency program participation; (ii) a publicly-available release form should be on the utility's website, to expedite the transfer of energy information; and (iii) customer utility data should be available in electronic, machine readable form. The Mission:data/AGO rule addresses each of these topics directly and in a manner that would satisfy Asheville's concerns. In addition, whereas it is unclear whether the Public Staff's draft rule would require the release of billing and account information that Asheville states is necessary to manage municipal facilities, the Mission:data/AGO rule is explicit and defines "standard customer data" to include "customer name, mailing address, premise address, any contact information, payment history, account number(s), and all information on bills including, but not limited to, line item charges and charge descriptions, amounts billed, the rate or tariff applicable to the account or meter, billing cycle dates, etc." Consequently, the Mission:data/AGO rule directly satisfies Asheville's concerns stated in initial comments.

6. **CONCLUSION**

WHEREFORE, the Mission:data Coalition respectfully requests that the Commission adopt the proposed rule proffered by it and the North Carolina Attorney General as new R8-51 in Chapter 8 of the Commission's Rules. In the alternative, if the Commission has any concerns regarding that proposed rule or requires further clarification as a result of issues raised by other parties in these reply comments, the Mission:data Coalition respectfully requests the opportunity to file sur-reply comments to address any outstanding concerns or issues.

Respectfully submitted this the 17th day of July, 2020.

/s/ Kurt J. Olson
Kurt J. Olson, Esq.
Counsel for Mission:data Coalition
State Bar No. 22657
P.O. Box 10031
Raleigh, NC 27612
(919) 916-7221
kurt.j.olson@gmail.com

CERTIFICATE OF SERVICE

I hereby certify that all persons on the docket service list have been served true and accurate copies of the foregoing by first class mail deposited in the U.S. mail, postage pre-paid or by email transmission with the party's consent.

Respectfully submitted this the 17th day of July, 2020.

/s/ Kurt J. Olson
Kurt J. Olson, Esq.
Counsel for Mission:data Coalition
State Bar No. 22657
P.O. Box 10031
Raleigh, NC 27612
(919) 916-7221
kurt.j.olson@gmail.com

APPENDIX A

Rule R8-51. CUSTOMER AND THIRD-PARTY DATA ACCESS and PRIVACY.

(a) Definitions.

(1) "Aggregated data" means usage data, alone or in combination with other data **s*u**ch as energy savings data at a premise*, from which sufficient identifying information has been removed such that an individual, family, household, residence, or customer cannot reasonably be identified or re-identified.

(2) "Application programming interface" or "API" means a utility's internet-based system that securely provides customer data to customer-authorized third-parties using machine-to-machine communications.

(3) "Authorized third party" means a third party that has received authorization from a customer to access, receive, collect, store, use, or disclose standard customer data and that obtains the information from a utility.

(4) The "Commission" is the North Carolina Utilities Commission.

(5) "Covered information" means any information that is "standard customer data," "unshareable personal data," or "usage data" as defined in this rule. Covered information does not include, however, aggregated data. Covered information also does not include information provided to the Commission pursuant to its oversight responsibilities.

(6) The "primary purposes" for the collection, storage, use or disclosure of covered information are to:

(i) Provide or bill for electrical power;

(ii) Provide for system, grid, or operational needs;

(iii) Provide services as required by state or federal law or as specifically authorized by an order of the Commission; or

(iv) Plan, implement, or evaluate demand response, energy management, or energy efficiency programs under contract with a utility, under contract with the Commission, or as part of a Commission-authorized program conducted by a governmental entity under the supervision of the Commission.

(7) "Secondary purpose or use" means any purpose or use that is not a primary purpose or use.

(8) "Standard customer data" means

(i) all energy usage data collected by a meter that a utility maintains as part of its regular records in the ordinary course of business, including kilowatt-hours used,

load profile, and, where applicable to certain rate classes, kilo-volt-amps, kilo-volt-amperes-reactive, power factor, and the like;

(ii) customer-specific information including customer name, mailing address, premise address, any contact information, payment history, account number(s), and all information on bills including, but not limited to, line item charges and charge descriptions, amounts billed, the rate or tariff applicable to the account or meter, billing cycle dates, etc.; and

(iii) any information that might be necessary for participation in, or to determine customer eligibility for, bill payment assistance, renewable energy, demand-side management, load management, or energy efficiency programs**.**

Standard customer data does not include unshareable personal data.

(9) "Unshareable personal data" means the birth date, social security number, biometrics, bank and credit card account numbers, driver's license number, credit reporting information, bankruptcy or probate information, health information, or network or internet protocol address of the customer or any person at the customer's location. This personal information is specifically excluded from the definition of standard customer data and, as stated in section (d)(9) of this Rule, will not be shared by a utility with any party other than the customer.

(10) "Usage data" is all energy usage data collected by a meter including but not limited to kilowatt-hours used, load profile, kilo-volt-amps, kilo-volt-amperes-reactive, power factor, kW, or voltage.

(11) For purposes of this rule, the word "utility" has the same meaning as is defined in Rule R8-2.

(12) For purposes of this rule, a "utility contractor" means any third party that provides services to a utility under contract with that utility.

TRANSPARENCY (NOTICE OF USE OF CUSTOMER INFORMATION)

(b) Notice.

(1) Generally. – Utilities shall protect covered information in their possession or control to maintain the privacy of customers. Utility contractors' permissible uses of data and obligations to protect data are governed by contract with the utility as set forth in section (d) of this rule.

(2) Notice Requirement. – Utilities shall provide customers with meaningful, clear, accurate, specific, and comprehensive notice regarding the accessing, collection, storage, use, and intentional disclosure of covered information. Utilities shall also provide such notice regarding the compilation, use, and disclosure of aggregated data.

(3) When Provided. – Utilities shall provide a written notice that meets the requirements of subdivision (b)(2) when confirming a new customer account, and at least once a year, utilities shall inform customers how they may obtain an updated copy of this notice. Utilities shall provide a conspicuous link to such notices under subdivision (b)(2) on the home page of their websites. Moreover, utilities shall include a link to the notice in all electronic mail to customers. Utilities shall also provide this notice upon request by any party.

(4) Form. – The notice, which may take the form of or be included in a privacy policy, shall be labeled "Notice of How We Gather, Use and Disclose Your Information" and shall:

(i) Be written in easily understandable language; and

(ii) Be no longer than is necessary to convey the requisite information.

(5) Content. – The notice shall state clearly:

(i) The identity of the utility;

(ii) The effective date of the notice;

(iii) The utility's process for altering the notice, including how the customer will be informed of any alterations and where prior versions will be made available to customers; and

(iv) The title and contact information, including email address, postal address, web address, and telephone number, of an official at the utility who can assist the customer with privacy questions, concerns, or complaints regarding the collection, storage, use, or disclosure of covered information or aggregated data.

The notice shall also:

(v) Include a description of the standard customer data made available to customers;

(vi) Indicate the frequency with which standard customer data can be provided;

(vii) Explain that disclosure of customers' data to third parties affects customer privacy, providing insight into their energy-consuming behaviors and permitting inferences about customers' daily activities, absences from the home or business, patterns of behavior, and lifestyle;

(viii) Explain that customers, before they authorize the disclosure of their data to third parties, should consider how the third party would be able to access and use their data;

(ix) Explain that the privacy and security of customer account and usage data will be protected by the utility while the data is in the utility's possession or control, but that the utility is not responsible for the privacy or security of the data after it has been transferred successfully to the customer or to an authorized third party;

(x) Identify any charges that may be applicable for customers to access data that are not standard customer data;

(xi) State that standard customer data will not be disclosed to third parties without customers' express, written consent in a manner and form approved by the Commission;

(xii) Explain the utility's policies regarding the manner in which a customer can authorize access and disclosure of covered information to third parties;

(xiii) Describe how the customer can terminate authorized third-party access to covered information; and

(xiv) Inform customers that covered information may be used to create aggregated data that will not contain customer-identifying information, and that the utility may provide such aggregated data to third parties subject to Commission Rule R8-51.

(xv) Explain that unshareable personal information will not be shared by a utility with any party other than the customer at any time.

(c) Purpose Specification. – The notice required under subsection (b) shall also provide:

(1) An explicit description of:

(i) Each category of covered information collected, used, stored or disclosed by the utility, and, for each category of covered information, the reasonably specific purposes for which it will be collected, stored, used, or disclosed.

(ii) Each category of covered information that is disclosed to third parties, and, for each such category:

(a) The purposes for which it is disclosed; and

(b) The categories of third parties to which it is disclosed.

(iii) The specific identities of those authorized third parties to whom data is disclosed for secondary purposes, and the secondary purposes for which the information is disclosed.

(2) The approximate period of time that covered information will be retained by the utility or utility contractor.

(3) A description of:

(i) The means by which customers may view, inquire about, or dispute their covered information; and

(ii) The means, if any, by which customers may limit the collection, use, storage or disclosure of covered information and the consequences to customers if they exercise such limits.

USE AND DISCLOSURE LIMITATION

(d) Use and Disclosure Limitations.

(1) Generally. – Utilities are authorized to use covered information to provide regulated utility service in the ordinary course of business. Providing such service is a primary purpose.

(2) No Sale of Customer Information. – Utilities may not sell information about customers or covered information, other than aggregated data, for consideration of any kind.

(3) Use of Covered Information by a Utility for Primary Purposes. – A utility may access, collect, store and use covered information without customer consent, provided the use is for primary purposes and no disclosure is made to a utility contractor except as allowed by section (d)(4) below.

(4) Disclosure by a Utility Without Customer Consent. – A utility may disclose standard customer data to a utility contractor without customer consent only:

(i) When explicitly ordered to do so by the Commission; or

(ii) For a primary purpose being carried out under contract with and on behalf of the utility disclosing the data; provided that the utility shall, by contract, require the utility contractor to agree to use the data only for the primary purpose and to access, collect, store, use, and disclose the information pursuant to policies, practices and notification requirements no less protective than those under which the utility itself operates as required under this rule, unless otherwise directed by the Commission. As part of this contractual agreement, utilities shall require utility contractors to provide similar contractual protections for standard customer data in the context of all subsequent disclosures for primary purposes.

(5) Terminating Disclosures to Entities Failing to Comply with Their Privacy Assurances. – When a utility discloses standard customer data to a utility contractor under this subsection (d), it shall specify by contract, unless otherwise ordered by the Commission, that it shall be considered a material breach if the contractor engages in a pattern or practice of accessing, storing, using or disclosing the information in violation of the party's contractual obligations to handle the information pursuant to policies no

less protective than those under which the utility from which the information was initially derived operates. If a utility determines in good faith that a utility contractor is in breach of its contract for this reason, the utility shall promptly cease disclosing the information to the contractor.

(6) Ban on ***Use or*** Disclosure [] Without Consent. – No utility shall use or disclose standard customer data to any party for any secondary purpose without obtaining the customer's prior, express, voluntary, authenticated authorization for each distinct secondary purpose. This authorization is not required when information is:

(i) Provided pursuant to a legal process;

(ii) Provided in situations of imminent threat to life or property; or

(iii) Specifically authorized by the Commission pursuant to its jurisdiction and control.

(7) Requirements for Authentications of Consent. Customer authorizations to disclose customer data are authenticated, under this Rule, if the customer's identity is established in either oral, electronic or non-electronic form and can be documented by the utility. Separate authorization by each customer must be obtained for all secondary uses of covered information by a utility.

(8) Form of Consent. – The customer consent form or process must be approved by the Commission, and shall include:

(i) Information to adequately identify the customer, consistent with, and no more onerous than, a utility's authentication practices when a customer creates an online account on a utility's website or when a customer calls the utility by telephone;

(ii) The intended purpose and the use of the data being requested;

(iii) The time period (e.g., months, years) during which the secondary use will take place;

(iv) The category of information to be shared, with a succinct description of each; and

(v) ***In the event the utility seeks to use customer data for a secondary purpose, a*** commitment to the customer that the utility shall be responsible for using the data only for the authorized ***purpose*** and that the utility will continue to protect the privacy and security of the data in accordance with this rule.

If a consent is made by electronic means, the information provided shall be in spoken form, displayed on a screen, or otherwise displayed to the customer via the customer's preferred contact method. If a consent is made by oral means, the information listed in sections (i)

through (iii) shall be obtained and provided in spoken form, but the commitment to the customer in section (iv) may be provided either in spoken form or by directing the customer to a website that provides the commitment to the customer.

(9) Ban on Disclosure of Unshareable Personal Data. – Nothing in this Rule shall allow, and utilities shall be prohibited from, providing unshareable personal data to any party other than the customer. However, network or internet protocol addresses may be shared by a utility to a utility contractor for a primary purpose.

CUSTOMER ACCESS AND CONTROL

(Individual Participation)

(e) Customer Access and Control.

(1) Quality and Quantity of Standard Customer Data. – A utility shall maintain at least 24 months of standard customer data, or the period of time that a customer has had an account at a given address, whichever is less, in sufficient detail for a customer to understand his or her energy usage. The frequency interval of data must be commensurate with the capabilities of the meter or network technology used to serve the customer.

(2) Customer Access to Standard Customer Data. – As part of basic utility service, upon request, a utility shall provide a customer access to the customer's own standard customer data provided in electronic machine-readable format, in conformity with nationally recognized standards and best practices concerning form and frequency, such as the latest version of the North American Energy Standard Board's (NAESB) Req. 21, the Energy Services Provider Interface (ESPI), and in a manner that ensures adequate protections for the utility's system security and the continued privacy and security of the customer data during transmission***, except if transmitted by email***.

(3) Cost. – When the data requested is standard customer data and the request pertains to a time period within the previous 24 months, the request for access will be fulfilled without charge. If requests are made for information other than standard customer data or data outside the 24 months preceding the request, and utilities seek to charge customers a fee to provide such data, the utility may charge an amount that the Commission deems reasonable based on the utility's marginal cost to provide those data.

(4) Control. – Customers have the right to share their own standard customer data with authorized third parties of their choice to obtain services or products provided by those third parties and to ensure accuracy of covered information held by utilities and utility contractors. Utilities shall provide customers with convenient mechanisms for:

(i) Granting and revoking authorization for secondary uses of standard customer data by third parties;

(ii) Disputing the accuracy or completeness of any covered information that a utility is storing or distributing for any primary or secondary purpose; and

(iii) Requesting corrections or amendments to any covered information that the utility is collecting, storing, using, or distributing for any primary or secondary purpose.

AUTHORIZED THIRD PARTY ACCESS
TO CUSTOMER DATA FROM A UTILITY

(f) Authorized Third Party Access to Standard Customer Data from a Utility.

(1) Third Party Access upon Customer Authorization. – For the period of time during which a customer has provided consent, utilities shall grant authorized third parties access to the customer's standard customer data in electronic machine-readable format, in conformity with nationally recognized standards and best practices concerning form and frequency, such as the latest version of the North American Energy Standard Board's (NAESB) Req. 21, the Energy Services Provider Interface (ESPI), and in a manner that ensures adequate protections for the utility's system security and the continued privacy of the data in transit from a utility to an authorized third party. ***Following receipt of a valid customer authorization as described below, utilities shall electronically deliver requested data to the third party within 90 seconds, unless the customer has requested data delivery by another method.***

(2) Customer Authorization. – Utilities shall designate the categories of standard customer data available to authorized third parties in conformity with this rule and provide brief descriptions of those categories in plain language for customers to understand. For all methods of authorization described below, when a customer authorizes third party access, the customer will identify the categories of information the customer wishes to share. If an authorized third party specifies the data it would like permission to access, the utility shall display such request to customers using the aforementioned categorical designations. Separate authorization by each customer must be obtained for all disclosures of standard customer data except as otherwise provided for herein.

(3) Authorization Process. – A utility shall not disclose standard customer data to a third party unless an authorization is valid as described in this rule. A utility shall, regardless of the authorization method described in this Rule, use consistent customer information to validate the customer's identity in a manner that is no more onerous than a utility's authentication practices when a customer creates an online account on a utility's website or when a customer calls the utility by telephone. A utility shall provide the following methods for any customer to grant a valid authorization: non-electronic; customer-initiated electronic; and at least one authorized third-party initiated electronic method using an API that is non-proprietary to the utility and is commonly used in the industry by other utilities.

(i) Non-electronic methods. Any customer may submit an authorization to a utility by at least the following methods:

(A) By telephone, in which authorizations shall be processed, and data transmitted, within one (1) business day; or

(B) By mail to a utility's mailing address, in which case authorizations shall be processed, and data transmitted, within one (1) business day.

(ii) Customer-initiated electronic methods. Any customer may submit an authorization to a utility by completing a web-based submission on a utility's website, consistent with nationally recognized standards and best practices. In this case, a utility shall allow direct online submission following completion without requiring email or an online account.

(iii) Customer-requested, authorized third party initiated electronic methods. A customer may interact directly with a third party and provide the third party with the customer's account number. The utility shall receive a customer's account number from the third party via API and seek authentication from the customer as well as customer consent via the customer's preferred contact method (such as by one-time passcode). Once authorized, the utility shall provide the requested data to the authorized third party via API. In this context, the utility will authenticate the customer's identity, process the request for access, and permit electronic authorization via API in a timeframe no longer than the time required for a customer to create an online account at a utility's website and access his or her standard customer data.

(4) Requirements of authorization. For all authorization methods used, a utility shall

(i) Enable and require the designation of the authorized third party and the customer;

(ii) Enable and require the specification of the purpose for sharing the data and the intended use of the data by the authorized third party;

(iii) Enable and require the designation of the time period (e.g., months and years of both historic and future data) for which data is being requested. The utility shall provide customers the option to authorize an ongoing provision of data that is valid until revoked by the customer or provision for a specified period of time.

(iv) Enable and require the designation of the categories of standard customer data being requested in accordance with (f)(2).

(v) Provide notice to the customer that, following access or transfer, the utility shall not be responsible for monitoring or ensuring that the third party to whom the data is disclosed is maintaining the confidentiality of the data or using the data as intended by the customer.

(5) Revocation and Termination. – Customers have the right to revoke, at any time, any previously granted authorization. Termination of electric utility service also terminates consent to disclose customer data granted by the customer for the meter(s) or premise(s) where electric utility service has been terminated. A utility shall also permit an authorized third party to terminate its authorization, in which case a utility shall subsequently notify a customer of the termination via the customer's preferred contact method and confirm to the authorized third party that the termination is accepted.

(6) Opportunity to Revoke. – The consent of a residential customer shall continue without expiration if the customer has elected ongoing provision until revocation, but the utility must contact a customer once annually to inform the customer of the authorization(s) granted and to provide an opportunity for revocation. The utility shall use electronic means to make this annual notice if the utility holds electronic contact information for the customer. The consent of a non-residential customer shall continue in the same way, but a utility must notify a non-residential customer once, upon an initial authorization, to provide an opportunity for revocation.

(7) Modifications. – Changes of contact names for an organization, trade name, or utility over time do not invalidate consent as to the respective organization, trade name, or utility. Modifications to the consent form or process over time do not invalidate previous consent.

(8) Parity. – Utilities shall permit customers to revoke authorization for any secondary purpose of their standard customer data by the same mechanism(s) initially used to grant authorization.

(9) Eligibility Determinations. – To protect the privacy and security of covered information, utilities shall apply eligibility criteria as follows. To be eligible to receive standard customer data, authorized third parties shall be required by utilities to: (1) demonstrate technical capability to interact securely with the utility's servers; (2) provide contact information and federal tax identification numbers to a utility; (3) acknowledge receipt and review of these privacy and access Rules; (4) not have been disqualified as an authorized third party provider in the past pursuant to processes outlined at (h)(2)-(4); and (5) adopt and comply with the most updated version of the 2015 Department of Energy's Voluntary Code of Conduct Final Concepts and Principles for Data Privacy and the Smart Grid (the "DataGuard Seal") or a similar nationally accepted eligibility standard approved by the Commission as a necessary, comparable, reasonable and appropriate alternative.

(10) Descriptive rate schedules. – A utility shall include in its rate schedules a description of standard customer data that it provide**s** to the customer, to an authorized

representative of the customer, or to an authorized third-party recipient. At a minimum, the utility's rate schedule must provide the following:

(i) A description of standard customer data and the frequency of updates that will be available;

(ii) The method and frequency of standard customer data transmittal and access available (electronic, paper, etc.), pursuant to which data is provided to authorized third parties as soon as practicable following collection of the usage data, as well as the security protections or requirements for such transmittal;

(iii) A reasonable timeframe for processing requests, consistent with this rule; and

(iv) A ***statement that no*** fees or charges ***will be*** associated with processing a request for ***standard customer*** data.

(11) Records of Disclosures. – The utility shall maintain records of all disclosures of covered information to third parties, including a copy of the customer's authorization to disclose standard customer data (unless it was in oral form) and a list of the information disclosed using the categories developed by the utility under section (f)(2) of this Rule. The utility shall maintain records of standard customer data disclosures for a minimum of three years and shall make the records of the disclosure of a customer's data available for review by the customer upon request.

LIABILITY AND COMPLAINTS

(g) Liability. – Nothing in this Rule shall be construed to impose any liability on a utility or any of its directors, officers and employees, relating to disclosures of information when 1) the Commission orders the provision of standard customer data to a third party; or 2) a customer discloses covered data to, or authorizes access to standard customer data by, a third party that is unaffiliated with and has no other business relationship with the utility. Specifically, after a utility securely transfers covered information to a customer or standard customer data to an authorized third party pursuant to a customer's request, nothing in this Rule shall make a utility responsible for the security of the information or its use or misuse by such customer or by a third party. This section does not apply where a utility has acted recklessly.

(h) Complaints.

(1) Complaints Submitted by Customers Against Utilities. Complaints from customers regarding a utility's failure to process customer authorizations to release standard customer data pursuant to this Rule in a timely and accurate manner, or to provide eligible authorized third parties with access to a customer's standard customer data in a timely and accurate manner, or regarding the utility's failure to comply with this Rule in any other respect, shall be treated as complaints under Rule R1-9.

(2) Complaints Submitted to a Utility. If a utility disclosing standard customer data to a Commission-authorized or customer-authorized third party receives a customer complaint about the third party's misuse of data, the utility shall keep records of such complaints and submit a report to the Commission annually of any such complaints or suspected violations. If a utility believes it is necessary to terminate an authorized third party's access to customer data, the utility shall file a request with the Commission in accordance with paragraph (h)(3).

(3) Complaints submitted by a utility. If a utility has a reasonable suspicion that an authorized third party has engaged in conduct rendering it ineligible to access information under this Rule, the utility shall expeditiously inform the Commission and the Public Staff of any information regarding possible ineligibility.

(4) If the Commission confirms that a third party is or has become ineligible to receive information as an authorized third party under this Rule, the Commission shall allow the utility to refrain from providing or to discontinue providing standard customer data to that party.

A utility will not be deemed to have made a reckless transmission of covered information to an authorized third party if the utility acts consistently with the process described in paragraphs (2) and (3) above.

A utility is prohibited from unilaterally revoking access to an authorized third party for any reason other than a ***Commission order pursuant to paragraph 4 above or a*** good faith belief that the third party poses an imminent danger to life, property or the cybersecurity of the utility's systems.

(i) Penalties. – An admission to or Commission adjudication of liability for a violation of these rules may result in an assessment of a civil penalty or fine as provided by 15 N.C. Gen. Stat. 62-310 et seq.

AGGREGATED USAGE DATA

(j) Aggregated Usage Data.

(1) Availability of Aggregated Usage Data. – Utilities may permit the use of aggregated usage data from which all identifiable information has been removed to be used for analysis, reporting or program management provided that the release of that data does not disclose or reveal specific customer information because of the size of the group, rate classification, or nature of the information.

(2) Requests for Aggregated Data Reports from a Utility. – A utility may disclose readily available aggregated ***monthly usage*** data that consists of at least fifteen customers, where the data of a single customer, or of premises associated with a single customer, does not comprise 15 percent or more of the aggregated data. In aggregating customer data to create an aggregated data report, a utility must ensure the data does not include any identifiable customer data. A utility shall not provide ***usage*** aggregated customer

data in response to multiple overlapping requests from or on behalf of the same requestor that have the potential to identify customer data.

(3) ***Requests for Aggregated Data for the purposes of building benchmarking. If a customer seeks aggregated data for a particular building for the purpose of benchmarking a building energy performance using the United States Environmental Protection Agency's EnergyStar ranking, then a utility shall timely fulfill requests for monthly aggregated usage data for that particular building or premises only. A utility shall offer such customer a limited nondisclosure agreement specifying that the customer may only use the aggregate usage data for the purposes of EnergyStar benchmarking and/or complying with a local municipal ordinance related thereto. If a customer executes said nondisclosure agreement, then a utility will provide monthly aggregated usage data for the building(s) requested provided that the aggregation consists of at least four (4) customers, where no single customer's usage exceeds fifty percent (50%) of the total over the course of 12 months.***

(4) Opportunity to Revise Requests. – If an aggregated data report cannot be generated in compliance with this rule, the utility shall notify the requestor that the aggregated data, as requested, cannot be disclosed and identify the reasons the request was denied. The requestor shall be given an opportunity to revise its aggregated data request in order to address the identified reasons.

(5) Rate Schedules. – A utility shall file for Commission approval to amend its rate schedules to include a description of aggregated data reports available from the utility. At a minimum, the utility's rate schedules shall provide the following:

(i) A description of the aggregated data reports available from the utility, including all available selection parameters (usage data or other data);

(ii) The frequency of data collection;

(iii) The method of transmittal available (electronic, paper, etc.) and the security protections or requirements for such transmittal;

(iv) The applicable charges for providing an aggregated data report;

(v) The timeframe for processing requests; and

(vi) A form for requesting an aggregated data report to the utility identifying any information necessary from the requestor in order for the utility to process the request.

REPORTING ON DISCLOSURES PURSUANT TO LEGAL PROCESS

(k) Disclosure Pursuant to Legal Process.

Except as otherwise provided in this rule, a court order, state or federal law, or by order of the Commission:

(1) Reporting. – On an annual basis, utilities shall report to the Commission the number of demands received for disclosure of customer data pursuant to legal process and the number of customers whose records were disclosed. Upon request of the Commission, utilities shall report additional information to the Commission on such disclosures. The Commission may make such reports publicly available without identifying the affected customers unless making such reports public affects or would affect an ongoing criminal investigation.

DATA MINIMIZATION

(l) Data Minimization, Generally. — Utilities shall collect, store, use, and disclose only as much covered information as is reasonably necessary or as authorized by the Commission to accomplish the reasonably specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

(m) Data Retention. – Utilities shall maintain covered information only for as long as reasonably necessary or as authorized by the Commission to accomplish a specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

(n) Data Disclosure. – Utilities shall not disclose to any third party more standard customer data than is reasonably necessary or as authorized by the Commission to carry out a specific primary purpose identified in the notice required under subsections (b) and (c) or for a specific secondary purpose authorized by the customer.

DATA QUALITY AND INTEGRITY

(o) Data Quality and Integrity. – Utilities shall ensure that covered information they collect, store, use, and disclose is reasonably accurate and complete or otherwise compliant with applicable rules and tariffs regarding the quality of energy usage data.

DATA SECURITY

(p) Data Security and Breach Notification.

(1) Generally. – Utilities shall implement reasonable administrative, technical, and physical safeguards to protect covered information from unauthorized access, destruction, use, modification, or disclosure.

(2) Notification of Breach. – Notwithstanding and in addition to any other legal requirements, a utility shall require a utility contractor providing services to a utility for a primary purpose to notify the utility that is the source of the data within one week of the detection of a breach. Upon a breach affecting 1,000 or more customers, whether by a utility or by a third party described herein, the utility shall notify the Commission

of security breaches of covered information within two weeks of the detection of a breach or within one week of notification by a third party of such a breach. Upon request by the Commission, utilities shall notify the Commission of security breaches of covered information.

(3) Annual Report of Breaches. – In addition, a utility shall file an annual report with the Commission, commencing with the calendar year 2021, that is due within 120 days of the end of the calendar year, and notifies the Commission of all security breaches within the calendar year affecting covered information maintained by a utility directly or through one of its contractors.

ACCOUNTABILITY AND AUDITING

(q) Utilities shall be accountable for complying with the requirements herein, and must make available to the Commission upon request or audit:

(1) The notices that they provide to customers pursuant to these rules.

(2) Their internal and consumer-facing privacy and data security policies.

(3) The categories of agents, contractors and other third parties to which they disclose standard customer data for a primary purpose, the identities of agents, contractors and other third parties to which they disclose standard customer data for a secondary purpose, the purposes for which all such information is disclosed, indicating for each category of disclosure whether it is for a primary purpose or a secondary purpose. (Utilities shall retain and make available to the Commission upon request information concerning who has received standard customer data from them.)

(4) Copies of any secondary-use authorization forms by which the utility secures customer authorization for secondary uses of covered data.

(r) Customer Complaints. – Utilities shall provide customers with a process for reasonable access to covered information, for correction of inaccurate covered information, and for addressing customer complaints regarding covered information under these rules.

(s) Training. – Utilities shall provide reasonable training to all employees and contractors who collect, use, store or process covered information.

(t) Audits. – Each utility shall conduct an independent audit of its data privacy and security practices in conjunction with general rate case proceedings following 2020 and at other times as required by order of the Commission. The audit shall monitor compliance with data privacy and security commitments, and the utility shall report the findings to the Commission as part of the utility's general rate case filing.

(u) Reporting Requirements. – On an annual basis, each utility shall disclose to the Commission, as part of the annual report required by Rule ___, the following information:

(1) The number of authorized third parties accessing standard customer data.

(2) The number of non-compliances with this rule or with contractual provisions required by this rule experienced by the utility, and the number of customers affected by each non-compliance and a detailed description of each non-compliance.