Exhibit:
Issues: Green Button Connect
Witness: Michael Murray
Type of Exhibit: Surrebuttal
Sponsoring Party: Renew Missouri
Case No.: ER-2024-0261
Date Filed: September 17, 2025

BEFORE THE MISSOURI PUBLIC SERVICE COMMISSION

FILE NO. ER-2024-0261

SURREBUTTAL TESTIMONY AND EXHIBITS OF MICHAEL MURRAY ON BEHALF OF RENEW MISSOURI

September 17, 2025

TABLE OF CONTENTS

I. PURPOSE OF SURREBUTTAL TESTIMONY AND SUMMARY OF RECOMMENDATIONS

Q. PLEASE STATE YOUR NAME, TITLE AND BUSINESS ADDRESS.

A. My name is Michael Murray. I am the President of Mission:data Coalition ("Mission:data"). My business address is 1752 NW Market Street #1513, Seattle, WA 98107.

Q. ARE YOU THE SAME PERSON WHO FILED DIRECT TESTIMONY ON JULY 2, 2025, AND JULY 21, 2025, IN THIS PROCEEDING?

A. Yes.

Q. WHAT IS THE PURPOSE OF YOUR SURREBUTTAL TESTIMONY?

A. My purpose is to respond to the rebuttal testimony of the Staff of the Missouri Public Service Commission ("Staff") with regard to Green Button Connect My Data ("GBC"). I respond to Staff witness Mr. Matthew W. Lucas regarding alleged cybersecurity risks and the need for a GBC tariff.

II. RESPONSE TO STAFF

Q. WHAT DID STAFF WITNESS MR. MATTHEW W. LUCAS STATE WITH REGARD TO GREEN BUTTON CONNECT AND CYBERSECURITY?

A. In rebuttal testimony, Mr. Lucas states "there are real cybersecurity concerns associated with GBC" because GBC "involves the direct connection of customers or their third-party

representatives to a utility's data systems through an Application Programming Interface ("API")."[1]

Q. DO YOU AGREE WITH MR. LUCAS ABOUT THE "DIRECT CONNECTION?"

A. Not entirely. While of course GBC involves an API connection to the utility, it is not accurate to suggest that GBC requires unfettered communication with Liberty's underlying customer information system or meter data management system. In fact, all GBC implementations I am aware of involve numerous separations of functions, with layers of security between each function. For example, the server that responds to API queries is separated from the rest of Liberty's enterprise billing system.

Let me explain in more detail. There are two important and related cybersecurity strategies associated with all implementations of enterprise software, including GBC: "least privilege" and "defense in depth." Least privilege is the idea that any server, such as the GBC server that provides APIs, should only be granted the bare minimum access rights needed to fulfill its function. That means the GBC server does not have open access to customer data, Liberty's customer information system, billing system or meter data management system. Rather, it has only limited access rights, such as the ability to send certain defined requests that are subject to customer authorization. All other communications are prohibited.

The second strategy, which is related, is called "defense in depth." This is analogous to medieval castles, where attackers must pass through independent layers, often concentric rings. For example, a moat, outer gate, inner gate and a donjon must each be breached in order to reach the king or queen. Similarly, Liberty's networked infrastructure can and should have its own

[1] *Rebuttal Testimony of Matthew W. Lucas*, 3:3-6.

layered defenses consisting of firewalls, discrete network zones and load balancers, each of which prevents unwanted traffic from penetrating into the network. Penetrating a single layer does not mean that an attacker has complete access to an underlying system.

Together, least privilege and defense in depth are used to regulate and manage network traffic flows to ensure that requests for data are individually valid and that the underlying systems are protected. Mr. Lucas's word "direct" does not reflect the layering, nor the restraints on network traffic imposed at each layer, of the security measures that are used in enterprise software deployments such as GBC.

Q. IN TERMS OF CYBERSECURITY RISK, HOW DOES GREEN BUTTON CONNECT COMPARE WITH OTHER ONLINE SERVICES LIBERTY PROVIDES TODAY?

A. GBC has a similar risk profile to Liberty's customer web portal today. The customer web portal is exposed to the internet, which means it needs to have protections against denial-of-service attacks. It also needs to have layered protections so that a customer paying his or her bill cannot get access to power plant controls. Finally, Liberty's web portal needs an identity and access management system so that legitimate customers are given access to their accounts, while impersonators are denied access.

GBC has a very similar profile. GBC requires customer consent, which means that a customer must be able to login to his or her online account. By using the same identity and access management system underlying Liberty's website, as well as the same protection against denial-of-service attacks, GBC does not add new risks in this area. Next, GBC servers fulfilling API requests are similar to the website servers fulfilling requests from customers such as requesting a bill in PDF or making a payment. The web server does not have unfettered access to the customer

information system or billing system; instead, it routes valid requests to intermediate servers that are cordoned off from the customer information system or billing system. Just as Liberty's website is delivered to customers with multiple layers of servers underneath it, GBC is implemented the same way. With GBC, any request for data that is not agreed to by the customer is denied. Any attempt to gain control of the GBC server providing API responses would not yield any benefit to an attacker because, thanks to layered defenses, it has no authority within the network to receive unconsented data.

Q. IS IT POSSIBLE TO HAVE ZERO CYBERSECURITY RISK?

A. For any networked system, no, it is impossible to bring the risk to zero.

Q. CAN CYBERSECURITY RISKS ASSOCIATED WITH GREEN BUTTON CONNECT BE SUCCESSFULLY MANAGED?

A. Yes, absolutely. The electric utility industry has ten (10) years of experience with secure implementations of GBC. Tens of millions of customers nationwide have the ability to share their energy usage and account information today. Over the past decade, there has never to my knowledge been a single instance of a cybersecurity breach affecting a utility that is in any way connected with GBC.

Q. WHAT ELSE DID STAFF STATE REGARDING GREEN BUTTON CONNECT?

A. Mr. Lucas cites Liberty's new billing system called Customer First. Given that Liberty has not been able to accurately bill customers, Mr. Lucas states that any labor dedicated to GBC at this time would mean an inappropriate of resources away from repairing the billing system.[2] Mr. Lucas

[2] *Id.* at 3:20-4:11.

also states that the GBC tariff I proposed should be considered after, not before, the infrastructure for GBC is in place.[3]

Q. WHAT IS YOUR RESPONSE?

A. Liberty's ongoing issues with its billing systems strongly support the Commission's consideration of the GBC tariff. While I agree that GBC implementation should be sequenced after the billing system is stabilized, it is important for the Commission to set performance expectations for GBC at the outset. For Liberty to contract with its vendors to offer GBC, it needs to know what the Commission's requirements are. Reversing this order would limit the Commission's oversight in this area because the Commission could only address performance expectations *after* the system design, architecture and support expectations were established and contracted. Even if it were even possible to make modifications at that point, they would most likely add unnecessary costs.

I strongly agree with Mr. Lucas that Liberty's billing system must be promptly fixed. But in the meantime, the Commission should set performance expectations for GBC. Once the improvements to the billing system are complete, then Liberty will be well-positioned to begin offering GBC with a high level of confidence and accuracy. I note that Section (e) of the tariff specifically addresses data quality and integrity. It requires Liberty to provide customer data via GBC that meets a "best available" standard, meaning that it (1) applies to the correct customer in question, (2) is correct and accurate to the best of the utility's knowledge at that time, and (3) is transmitted in a timely manner to third parties. Certainly, customer bills should meet this standard. But so should GBC. The best way to ensure that outcome is for the Commission to take up the tariff and make determinations about performance expectations while the billing system improvements are underway.

[3] *Id.* at 6:12-16.

III. CONCLUSION

Q. DOES THIS CONCLUDE YOUR TESTIMONY?

A. Yes.

BEFORE THE PUBLIC SERVICE COMMISSION
OF THE STATE OF MISSOURI

In the Matter of the Request of The Empire District Electric Company d/b/a Liberty for Authority to File Tariffs Increasing Rates for Electric Service Provided to Customers In its Missouri Service Area	)))))	**File No. ER-2024-0261** Tracking No. JE-2025-0069

AFFIDAVIT OF MICHAEL MURRAY

STATE OF WASHINGTON)
) **ss**
COUNTY OF OKANOGAN)

COMES NOW Michael Murray, and on his oath states that he is of sound mind and lawful age; that he prepared the foregoing surrebuttal testimony; and that the same is true and correct to the best of his knowledge and belief.

Further the Affiant sayeth not.

M E Murray

Michael Murray

Subscribed and sworn before me this 10th day of September 2025.

Jesseca S Reece

Notary Public

NOTARY PUBLIC
STATE OF WASHINGTON
JESSECA S REECE
MY COMMISSION EXPIRES
JANUARY 18, 2029
COMMISSION # 189859

My commission expires: 01/18/2029

1