BEFORE THE PUBLIC SERVICE COMMISSION

OF THE STATE OF MISSOURI

Jonathan Miller,

Complainant,

v.

Spire Missouri Inc. d/b/a Spire,

Respondent.

File No. GC-2026-0007

COMPLAINANT'S EXCEPTIONS TO STAFF REPORT

COMES NOW the Complainant, **Jonathan Miller**, and files these Exceptions to the Staff Report submitted on **October 21, 2025** (Filing #64), in the above-referenced matter, pursuant to Commission Rule 20 CSR 4240-2.070(15)(B), and requests the Commission reject the Staff's finding of "no violations" and order appropriate **systemic remedies** in the Final Order for the protection of the public.

I. EXCEPTION: STAFF ERRED IN FINDING "NO VIOLATIONS" REGARDING DATA SECURITY

The Staff Report confirms that while complying with a discovery request, Spire "inadvertently sent another customer's recorded phone calls to Mr. Miller... [containing] sensitive information including account numbers, credit card information, account balances and the name of the customer and his wife along with their address"[11]. Staff concluded that Spire "violated no provisions" because the disclosure involved only one customer[2222].

The Complainant excepts to this finding:

1. **Setting a Dangerous Precedent:** The finding of "no violation" condones the unauthorized disclosure of private, financial, and identifying information (including credit card data) to a third-party litigant. This conclusion sets a **dangerously low security standard** that puts all Spire customers at risk.
2. **Requested Relief:** The Complainant requests the Commission find that Spire violated its fundamental duty to maintain the confidentiality and security of customer data, and issue an Order to establish a higher, enforceable legal standard for all utilities regarding unauthorized disclosures of sensitive customer data.

II. EXCEPTION: STAFF ERRED IN FINDING THE ISSUES WERE ISOLATED "ONE-OFFS"

Staff concluded that the multiple errors were "operator errors" and "one offs" that did not result from "system-wide causes"[3]. The Complainant excepts, arguing that the Report itself documents a **systemic failure** via the aggregation of critical errors and dangerous policies:

1. **System Vulnerability (Single Keystroke):** The account was "inadvertently placed on a budget plan when a Spire Customer Service Representative ('CSR') accidently hit a wrong button"[4]—a failure of system design that allows a critical account change from a single keystroke[5].
2. **Systemic Access Control Failure (SSN Policy):** Spire has indicated its internal policy allows a non-account holder to fully access and act on the account by providing only the "last four digits of the account holder's Social Security number"[6]. This policy provides insufficient security, violating modern standards for **PII (Personally Identifiable Information)** protection. The ability to gain full access using such minimal verification is a **failure of systemic policy**, not merely a CSR error.
3. **Data Security Breach:** The unauthorized disclosure of a third-party customer's highly confidential file[7777].

These three distinct failures collectively demonstrate a **systemic vulnerability** in Spire's account management software and security protocols, which must be addressed at the policy level.

III. EXCEPTION: THE RECOMMENDED REMEDY IS INSUFFICIENT TO PROTECT THE PUBLIC

Staff's recommendations rely entirely on providing "additional training"[8888]. The Complainant argues this is an inadequate, temporary remedy that fails to address the two primary, distinct systemic failures:

1. **Misinformation and Inadequate Service:** The Complainant was repeatedly provided with **inaccurate and conflicting information** from both **Spire CSRs** and **Commission representatives** regarding the CWR budget plan link[9]. This failure demonstrates a fundamental lack of control over standardized information dissemination, indicating a pervasive failure to provide **adequate and reliable service** as required by law.
2. **Training is Temporary, System Changes are Permanent:** Training will not eliminate the technical vulnerability that allows a single accidental keypress to make a critical account change. A technical solution is required to provide **long-term, public protection** against future human error.

Requested Systemic Remedies

The Complainant requests the Commission reject "training" as the sole remedy and enter a Final Order that mandates the following **systemic and public-protective actions**:

- **Technical System Change:** Mandate that Spire immediately update its customer management software to require **a mandatory two-step confirmation** (e.g., an "Are You Sure?" prompt) for any critical account change, specifically including budget plan enrollment.
- **Systemic Policy Change (SSN Security):** Mandate that Spire **cease using the last four digits of a Social Security number** as the sole or primary security credential for sensitive account actions.
- **System-Wide Audit:** Order the Commission's Staff to initiate a **system-wide audit** of Spire's IT security and internal controls to identify and close all vulnerabilities that allow for the "operator errors" documented in this case.

WHEREFORE, Complainant Jonathan Miller respectfully requests the Missouri Public Service Commission reject the Staff's finding of "no violations" and "one-offs," and enter a Final Order that mandates the immediate technical and systemic changes requested above to protect the public interest.

Respectfully submitted,
Jonathan Miller, Complainant Pro Se
[redacted]
[redacted]
Phone: [redacted]
Email: [redacted]

October 22, 2025

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing **Complainant's Exceptions to the Staff Report** has been served via electronic mail to all counsel of record listed on the official Docket Sheet this **22nd** day of **October**, 2025.

To:	**Counsel of Record for Spire (Respondent)**
Name:	[redacted]
Email:	[redacted]
To:	**Counsel for Staff**
Name:	[redacted]
Email:	[redacted]
Name:	[redacted]
Email:	[redacted]

Jonathan Miller

Complainant Pro Se