FORENSIC STATEMENT

Case No. EC-2026-0004
Brett Felber (Complainant) v. Ameren Missouri (Respondent)

I. Standard Banking Practice for Statements and EFT Traces

1. PDF Issuance – Banks, whether personal, commercial, small business, or corporate treasury, issue account statements, ledgers, and EFT traces exclusively in finalized PDF format or hardcopy statements derived from those PDFs.

2. Secure Access – Customers typically retrieve these documents through secure online banking portals or receive them via encrypted channels or postal delivery. The formatting is standardized, non-editable, and bears identifiers such as account numbers, bank branding, and date/time stamps.

3. NACHA & SWIFT Transmission Standards – NACHA requires EFT entries and traces to be exchanged between financial institutions using standardized ACH file formats. Customer-facing confirmations are issued as PDF notices, not code or editable generator files. SWIFT requires financial messages (e.g., MT103, MT202, ISO 20022 XML) to be delivered through the SWIFT network. Customer-facing confirmations are provided as PDF copies or authenticated message extracts, not in scripting language.

II. What Banks Do Not Do

1. Banks do not deliver records in Python code form. Python (.py files or Python-generated PDFs) is a programming language environment used by developers, not a banking document standard. If a “bank statement” exhibits metadata or structures consistent with Python libraries (e.g., ReportLab, FPDF, PyPDF2), it is a strong indicator the document was generated outside official banking systems.

2. Banks do not deliver editable or generator-created PDFs. Genuine bank PDFs are flattened, finalized files. They do not include markers of editing or portable document generation tools used by third parties. Artifacts such as “Created with Python PDF library” or “Editable layers” are forensic red flags indicating manipulation.

III. Forensic Conclusion

Based on these industry practices and forensic observations: Any document provided by Ameren Missouri in this case that claims to be a “bank statement” or “EFT trace” but contains Python-generated metadata or editable-PDF signatures is not authentic and should be deemed counterfeit, altered, or manipulated. This conclusion is supported by NACHA rules, SWIFT messaging standards, and ordinary banking practices, all of which dictate that customer-facing statements and EFT confirmations are issued strictly in PDF form or authenticated message format.

IV. Fiduciary & Statutory Duty

As a professional in the forensic analysis and mitigation industry, I have a statutory and fiduciary duty to report counterfeit or manipulated documents. Commission proceedings do not exempt Respondent from compliance with federal and banking standards. Any refusal by Respondent to produce authentic PDF banking records directly from the issuing institution, under NDA or protective order if necessary, further supports the conclusion that the prior exhibits are counterfeit.

V. Conclusion

The Respondent’s exhibit cannot be treated as authentic evidence because it was not generated according to banking industry standards. Banks do not issue customer documents in Python or editable-PDF form. Authentic statements and EFT traces are issued only in secured PDF formats or authenticated message extracts. Therefore, the Respondent’s exhibit is forensically invalid and should be stricken absent independent bank verification.

Respectfully submitted,

/s/ Brett Felber
Complainant
[redacted]

Dated: September 19, 2025