Date Filed: August 14, 2026

Witness: Jared A. Lawrence and Timothy W. McGrath
Request from: Office of Education, Outreach, and Enforcement

Question:

(ACCOUNT ESTABLISHMENT-FRAUD PREVENTION) Identify and describe all internal controls in place to prevent fraudulent account establishment, including accounts opened by telephone. For each control identified, explain:

a. Whether the control is preventive or detective;
b. Whether it is automated or manual;
c. When in the account establishment process the control is applied;
d. Whether the control is mandatory or may be overridden; and
e. Identify any circumstances under which an account could be established using only a customer's name or otherwise incomplete identifying information and explain the controls that would detect or prevent that occurrence.

Response:

The Company takes measures to ensure the security of customer information and identity theft protections are maintained for all customers.

Guidelines for protecting the confidentiality of Customer information are maintained in Company information systems and the conditions under which it can be released are defined in the Company's **160.3 Customer Confidentiality** policy (Exhibit CLP-REVREQ-2, Sch H-2.0 (F) at 15-16).

> *Before discussing any information with a purported Customer of record or their designee, the caller must first identify themselves as the Customer or their designee and provide adequate identifying data, in accordance with the Company's Identity Theft prevention guidelines.*

Guidelines designed to *detect, prevent, and mitigate identity theft* in connection with new or existing residential and certain commercial utility accounts are defined in **250.3 Identity Theft** policy (Exhibit CLP-REVREQ-2, Sch H-2.0 (F) at 35-36).

> *Customer Service Representatives ("CSRs") must reasonably validate the information provided by an individual regarding a new or existing account. If there is any suspicion or uncertainty regarding the individual's identity, a Red Flag alert shall be created and noted. Further attempts to validate the identity must be made prior to processing the individual's*

request. The CSR must refer to the Red Flag List and the defined procedures to address the situation.[1]

These controls are *both* preventive and detective.

Customer identification is required to start electric service with Eversource. When a customer provides their Social Security Number ("SSN") for identification purposes when establishing service, CSRs attempt to match their SSN to the customer's name using Experian. This verification process is *automated*, built directly into the customer information platform.

If the SSN cannot be verified to the customer, an additional step is taken to validate the information through a separate system called Lexis Nexis. When the SSN is unable to be matched on either platform, the customer is required to submit two forms of identification, one being a valid photo identification, via Eversource's secure document upload at Eversource.com. This process is *manual*.

Customers can also start service with other identification beyond the SSN. This verification process is *manual*.

Customers can also start service on Eversource.com. When customers navigate to "Request New Service" and enter their new service address, they're informed of "What You'll Need to Start Service" on the web and the list includes: SSN, email, and phone number. The same ID verification process is *automatically* conducted. This control *cannot* be overridden.

Customers *cannot* establish new service in the IVR.

While ID verification is mandatory for establishment of service, the Company does have guidelines for providing customers with *conditional* service when a customer establishes service at a location where the meter status is *on*. The customer is provided with conditional service for 30 days, pending receipt of valid identification. If valid identification is *not* received the metered service will be disconnected. The Company tracks and can identify customers who start conditional service by means of a Red Flag profile, as known as an alert, and an account note.

The Red Flag alert is also used for instances where a customer has reported potential concerns, as mentioned in CS Policy 250.3 above. Here, the CSR process becomes *manual* and again *cannot* be overridden.

[1] "Red Flags" shall mean those risks to Utility customer accounts indicated by patterns, practices or activities that indicate the possibility of identity theft that have been identified and incorporated into the Program.