Date Filed: August 21, 2026

Witness: Jared A. Lawrence, Jessica B. Cain, Timothy W. McGrath and Daniel M. Traynor
Request from: Office of Education, Outreach, and Enforcement

Question:

(FREQUENCY AND TRACKING OF FRAUDULENT ACCOUNTS) Provide, for each year from 2018 to present, the number of customer accounts identified as fraudulent, including those resulting from identity theft or insufficient identity verification at account creation. Please also describe how the Company tracks and categorizes such incidents internally.

Response:

Please refer to Table 1 below for the requested information regarding the number of customer accounts identified as fraudulent due to identity theft each year from 2018 to July 2026 in the table below.

Table 1. The number of customer accounts identified as fraudulent (Identity Theft)

Year	Number of Customers
2018	122
2019	93
2020	77
2021	52
2022	54
2023	70
2024	43
2025	30
2026	7

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 customer service policy **160.3 Customer Confidentiality** (Exhibit CLP-REVREQ-2, Sch H-2.0 (F) at 15-16), which states, in part:

> *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 the Company's customer service policy **250.3 Identity Theft** (Exhibit CLP-REVREQ-2, Sch H-2.0 (F) at 35-36), which states, in part:

> *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.*

Company Customer Service Representatives place a Red Flag alert when customers call the Company to report their personal information has been fraudulently used to establish service with Eversource.

When the Company processes the identity theft claim, a subsequent identifier is placed on the account that is then tracked in the Company's internal systems.