STATE OF CONNECTICUT
PUBLIC UTILITIES REGULATORY AUTHORITY

RE:	**INVESTIGATION INTO**	**:**	**DOCKET NO. 26-04-06**
	OF EVERSOURCE COMPANIES	**:**	
	DATA BREACH OF CUSTOMER	**:**	
	INFORMATION	**:**	**NOVEMBER 13, 2026**

REPORT OF THE OFFICE OF CONSUMER COUNSEL CONCERNING EVERSOURCE ENERGY'S DATA BREACH

The Office of Consumer Counsel ("OCC") respectfully files with the Public Utilities Regulatory Authority ("Authority") this Report regarding its investigation into the data breach of the Connecticut Light and Power Company and Yankee Gas Services Company, both d/b/a Eversource Energy ("Eversource"). The evidence indicates that Eversource released: customers' personal data, including their Social Security numbers and those of their family members; their family's income information; customers' contact information; and customers' government benefits information. Eversource did not identify the recent cyberattack until almost two weeks after it occurred and allowed the attacker to download more than 3.6 million files, many of which the attacker continued to download for three more days after Eversource was notified of the attack. Eversource then significantly delayed conveying the threat to its employees and the affected customers. Eversource's handling of this data breach causes grave concerns regarding its cybersecurity systems and processes, its ability to protect the information its customers entrust to it, and its willingness to timely and transparently communicate with its customers and employees.

On April 14, 2026, a cyberattacker infiltrated Eversource through one employee. Response to OCC-41; Correspondence dated August 26, 2026, p. 1. Three days later, on April 17, 2026, the cyberattacker continued this infiltration through a second employee. Response to OCC-42 ("On April 17, 2026, unauthorized access attempts were first detected on Employee 2's account,"). It was not until April 27, 2026, thirteen days after the initial attack, that Eversource became aware of the attack, and then only when it was contacted by the attacker. Response to OCC-30; Response to OCC-41 ("2026-04-27-10:18 – Employee 1's account was used to send the notification email."); Response to OCC-50. From April 14 through April 30, the attacker downloaded more than 3.6 million Eversource files (almost 2.5 million of them unique files). Responses to OCC-87, OCC-41, OCC-42. From April 27 (once Eversource was aware of the attack) through April 30, the attacker continued to access a significant number of additional files. Response to OCC-42, Attachment 1;[1] Response to OCC-77. On May 5 and May 6, 2026, the attacker attempted to gain continued access to files through at least two other employees. Responses to OCC-43 and OCC-44. On May 6, the cyberattacker emailed Eversource from Employee 4's email, again calling Eversource's attention to the attacker's continued access to Eversource's systems. Response to OCC-44 ("2026-05-06-14:13 - An email from the attacker sent from the employee's email address

[1] The Confidential Response to OCC-42, Attachment 1 shows the number of files downloaded on April 28 alone, which was a day after the attacker had already alerted Eversource to the attack.

without their knowledge was received by several corporate security distribution lists originating from Employee 4's account."). On May 22, Eversource issued a press release and informed its employees of the attack. Correspondence dated August 26, 2026.

I. Eversource released customers' personally-identifiable information.

Eversource released the personally-identifiable information of 2,592 Connecticut residents. Response to OCC-35; Correspondence dated August 26, 2026, p. 8. OCC has reason to believe the documents that the attacker accessed included customers' tax returns, bank statements, government benefits letters, and paycheck stubs, among other personal documents. *See* Response to OCC-60, Attachment 2, p. 4 (from Docket No. 26-05-01, Motion No. 7, Joint 03 – How It Works: Financial Hardship Verification).[2] This means that the documents not only contained the customer of record's personal and financial information, the documents likely contained personally-identifiable information about their family members, including children. Worse, this is the personal information of financial hardship customers, a vulnerable population that must trust Eversource with their personal data so they can receive help affording ever-increasing electric and gas bills. As a result of this data breach, entire low-income families have been placed at risk of having their lives altered through identity theft. It is possible that the "nature of this incident was that of a relatively narrow incursion without impact to electric or gas service, nor any intrusion into customer information systems or other critical operational systems or infrastructure," but not a single word in Eversource's attempt to downplay this event acknowledges the lives of the 2,592 Connecticut residents whose data Eversource failed to protect. Correspondence dated August 26, 2026, p. 1.

II. Eversource learned of the attack because it was contacted by the attacker and then failed to act quickly to prevent further loss of files

The evidence indicates that the cyberattack began on April 14, 2026. *Id.* at p. 3; Response to OCC-41. Eversource did not identify the attack until April 27, 2026, almost two weeks after it began. Correspondence dated August 26, 2026, p. 1; Response to OCC-41. It is generous, however, to state that Eversource "identified" the attack. Eversource became aware of the attack only because the attacker sent Eversource an email alerting it to the attack. Response to OCC-41 ("The email communications from the attacker using the employee's email address was the first time the Company became aware that Employee 1's account had been compromised by the attacker."). Had the attacker not sent that email, all parties are left to wonder when or even if Eversource would have identified the attack or known that its files had been accessed by an outside entity. As Eversource explained, these varied files were on a cloud server, not in an Eversource-owned system, which was the cause, though a poor excuse, for Eversource failing to identify the data breach until alerted by the attacker. Response to OCC-30.

During this initial thirteen-day window in which the attacker accessed Eversource's files unbeknownst to Eversource, the evidence indicates cyberattacker accessed almost 3 million

[2] These are the types of documents customers submit to verify their eligibility for a financial hardship designation. Despite repeated interrogatories requesting the specific documents the attacker accessed, Eversource indicated that it still does not know the specific documents or specific document types accessed. Responses to OCC-82, OCC-60, OCC-45, OCC-30.

Eversource files. Response to OCC-41 (noting the logs reflect from Employee 1's breach: 233,081 files accessed on April 14; 247,519 files accessed on April 15; 200,149 files accessed on April 16; 252,665 files accessed on April 17; 276,719 files accessed on April 18; 295,535 files accessed on April 19; 284,001 files accessed on April 20; 276,092 files accessed on April 21; 262,860 files accessed on April 22; 304,995 files accessed on April 23; 261,106 files accessed on April 24; and 33,239 files accessed on April 25); Response to OCC-42 (noting from Employee 2's breach "the logs reflected that approximately 720,000 files were downloaded over a 12-day period"). Both the length of time the cyberattacker had unnoticed access to Eversource's system and the number of files it accessed during this time is staggering.

More concerning, however, is the fact that Eversource *did not immediately stop the cyberattackers' file access* once it became aware of the attack. This indicates either a lack of capacity to protect its own system or a lack of seriousness concerning cybersecurity issues, or both. The attacker alerted Eversource to the breach on April 27, but the evidence indicates that the attacker continued to use its initial breach mechanisms to access Eversource files through April 30. Responses to OCC-42 and OCC-77. For another three days after the attacker alerted Eversource that it had breached Eversource's files, Eversource failed to prevent the attacker from downloading *additional* files. Response to OCC-77 ("Evidence indicates that the attacker group downloaded files using Employee 2's account from April 27, 2026 to April 30, 2026."); Response to OCC-42, Attachment 1 (indicating all downloads occurring on April 28). Over the course of its access through April 30, the cyberattacker accessed more than 3.6 million Eversource files, of which almost 2.5 million were unique. Response to OCC-87

Under such circumstances, it is no surprise that the attacker again breached Eversource's system a week later, on May 5, 2026. Response to OCC-43. Despite being aware of a cyberattack for more than a week, Eversource could not prevent the attacker from again gaining access to its system for *more than eight hours*. *Id*. (noting "a successful Software OATH MFA login at 2026-05-05 – 15:07, the addition of an alternate phone number at 15:09 and successful SMS logins at 15:10" and "2026-05-05-23:48 - Employee 3's account was locked."). Although Eversource states that "The attack on Employee 3 was detected by a newly created detection rule," this detection rule took more than one-third of a day to work. *Id*. Moreover, although Eversource claimed it did not observe files being downloaded through Employee 3, there is a marked difference between "no observed data exfiltration" and no data exfiltration. *Id*. In short, Eversource's interrogatory responses do not guarantee that the attacker did not continue to download files during the May 5 breach associated with Employee 3.

Only a day later, it happened again, except this time Eversource did not identify the attack itself and again learned of the attack because the attacker alerted it. On May 6, 2026, the attacker contacted Employee 4, who entered their credentials into an illegitimate website at the attacker's prompting. Response to OCC-44. For approximately one hour, the attacker again had access to Eversource's system. *Id*. (noting at 2026-05-06-13:50 the employee entered their credentials into the illegitimate website and at 2026-05-06-14:49 "Employee 4 password was reset, MFA session tokens revoked and computer locked down"). Even by the fourth attack, Eversource still took 36 minutes to disable the attacker's access after receiving the email from the attacker alerting it to the attack. *Id*. (noting Eversource received the email from the attacker at 2026-05-06-14:13 and locked

down Employee 4 at 2026-05-06-14:49).[3] Worse, even by the fourth attack, the attacker's access was limited to one hour solely because the attacker emailed Eversource from Employee 4's email alerting Eversource that it had accessed the system again. *Id*. ("2026-05-06-14:13 - An email from the attacker sent from the employee's email address without their knowledge was received by several corporate security distribution lists originating from Employee 4's account.).

Furthermore, evidence indicates Eversource *still* does not have a full picture of how the data breach occurred. Eversource admitted that it does not know how the cyberattacker triggered a valid Microsoft Authenticator notification for Employee 2. Response to OCC-76 (indicating Eversource presumed the cyberattacker must have had Employee 2's log in credentials, but despite investigation "The security team reviewed Employee 2's work email history and was not able to ascertain how the attacker had received the credentials that led to the MS Authenticator notification for this employee."). Moreover, Eversource indicated that it does not maintain a public-facing directory of employee email addresses, work phone numbers, or cell phone numbers and "The Company's investigation has not yet confirmed how the hacker group obtained employee information for the first of the four employee incidents." Response to OCC-7; Response to OCC-8. "Employee 4 was contacted by a phone call with a corporate phone number," therefore, the attacker apparently still has the ability to spoof Eversource phone numbers, and evidence indicated that "some employees received text messages on their personal phones that were part of the phishing attack." Response to OCC-44; Response to OCC-1. Eversource further indicated a month and a half after the attack that "it is not clear how many other employees may have received the phishing/smishing/vishing attack…" Response to OCC-1 (filed on June 1, 2026). Eversource continues to have significant gaps in its knowledge of what occurred, making it difficult to fully protect its systems from another attack.

Most alarming, the first two attacks were known only because the attacker alerted Eversource to them. The third attack was found only because a detection rule was established after the attacker alerted Eversource to the first two attacks. Then a fourth attack again was unknown until the attacker alerted Eversource to it. Had the attacker been less interested in ransom and more interested in secretly accessing files, parties are left to wonder if Eversource would be aware of the data breach even today.

III. Eversource did not quickly alert its employees to the cyberattack to prevent further breaches.

The evidence does not indicate that Eversource communicated to all of its employees that it had been the victim of a cyberattack. The Response to OCC-47 and associated attachments provide every communication to employees regarding the cyberattack. Only OCC-47 Attachment 16 mentions unauthorized access to data and the Authority should note the date of that communication and the limited audience to whom it was sent.[4] *See also* Response to OCC-47,

[3] It is curious that Eversource locked down Employee 1's account within 12 minutes of receiving the email (Response to OCC-41, email sent at 2026-04-27-10:18 and account locked at 2026-04-27-10:30), but a week into the attack it took three times as long to lock down Employee 4's account.

[4] The entirety of every OCC-47 communication is redacted, including the dates, so OCC will not publicly refer to this communication's date. It was not solely internal Eversource communications that were protected, but some communications that were sent to numerous outside vendors were also filed fully confidentially. OCC further invites

Attachment 1 (showing the audience for every communication and the date sent); Response to OCC-85 ("The first communication to the general employee population regarding the specific attack was issued on May 22, 2026.").

For the average worker, there is a difference between communications warning of generic threats or trainings regarding practices like phishing versus a communication from management directly saying the Company has been hacked. To find the difference, the Authority need look no further than the events that are the subject of this investigation. Eversource knew of the data breach on April 27. Despite that, employees continued *responding to* the attacker on May 5 and 6, more than a week later. On May 5, Employee 3 received a call from a random number, answered, and believed the random number to be "someone claiming to be support." Response to OCC-43. As a result, Employee 3 "entered information into what Employee 3 thought was a Copilot chat prompt at the caller's instruction." *Id*. The same occurred with Employee 4 on May 6. Having so little information from the Company about the cyberattack on May 6, "Employee 4 thought they were responding to Company efforts to protect the network." *Id*. Although Eversource claimed it was communicating with employees "who had a 'need to know'," the evidence indicates that Eversource underestimated the number of employees who needed to know and that underestimation caused further attacks. Response to OCC-85.[5]

Eversource then provided employees with a webinar on June 15. Response to OCC-62. First, this meeting was with employees at manager level or above, not every employee. *Id*. Second, the meeting was held 62 days after the attack began. A meeting with only upper-level employees held two months after the attack can hardly be termed a timely or comprehensive disclosure.

Honest and timely communication with employees creates an environment where employees are more vigilant against attacks. The result of piecemeal disclosures and attempts to downplay are seen here, where more employees and files are unnecessarily left vulnerable to further attacks.

IV. Eversource did not quickly or sufficiently alert its customers that it leaked their data.

As indicated, Eversource was made aware on April 27, 2026, that the attacker accessed the personally-identifiable information of 2,595 Connecticut residents. Response to OCC-35; Correspondence dated August 26, 2026, p. 8. Eversource sent a letter to customers regarding this leaked data on May 27, 2026, one full month after being aware that customers' personal data was in the hands of a group of criminals. Response to OCC-20, Attachment 1; Correspondence dated August 26, 2026, Appendix 1. Eversource explained that it stores the hardship documents that contained the personally-identifiable information in its system with the customer's account number

---

the Authority to compare the protected Response to OCC-47, Attachment 16, with the press release issued on the same day and filed publicly as the Response to OCC-75, Attachment 1.

[5] Eversource states that the attack was the subject of "an open federal law enforcement investigation," but does not state that the federal law enforcement prevented Eversource from disclosing the attack to employees. Response to OCC-85. If Eversource is stating that the federal government specifically instructed it not to tell its employees about the attack, Eversource will need to produce more than vague implications contained in an afterthought to an interrogatory response.

as the file name, meaning once Eversource saw which files were downloaded, it should have immediately known which customers were impacted. *See* Response to OCC-33; Response to OCC-36. Despite this, Eversource did not engage IDX until May 14, two and a half weeks after it was aware that the cyberattacker had accessed customers' information. Response to OCC-72. It then apparently took IDX another two weeks to determine the current addresses of the affected customers, a lengthy amount of time considering most of the active customers likely still live at the address Eversource has associated with their account. *See* Correspondence dated August 26, 2026, p. 8.[6]

Eversource sent the communication to customers one week after it issued a press release regarding the data breach. *See* Response to OCC-75, Attachment 1; Response to OCC-20, Attachment 1. As a result, Eversource had the opportunity in the press release to fully explain the implications of the data breach, yet it failed to do so. Instead, the press release downplayed the attack and overstated Eversource's response. Response to OCC-75, Attachment 1 (stating, "The activity was promptly identified and blocked…" but failing to state the data breach was identified solely because the attacker identified it for Eversource thirteen days after the initial attack, a reframing so generous that it calls into question the accuracy of the press release,). The press release included a buried line in the third paragraph stating, "some of the Company data accessed included personal information associated with approximately 3,049 former or current customers or household members," but made sure to immediately follow that line by explaining this represented "a very small percentage of our more than 4.6 million customers across our three-state territory." *Id*. In the fourth paragraph it stated, "Customers who may have been affected will receive direct notification with additional information and enrollment instructions," but it failed to state when or in what form, and it failed to state that all of the affected customers were customers with a hardship designation. *Id*.

This press release was particularly important due to the category of impacted customers and the timing. Customers with a hardship designation become eligible for service termination beginning on May 2 each year, causing many hardship customers to receive a variety of communications from Eversource around that time of year regarding enrolling on a payment arrangement and trying to prevent service termination. Yet another communication in the mail from Eversource on May 27 might be ignored without more preparation and context for the importance of the communication. Had Eversource prioritized protecting these customers, the press release would have focused on them and Eversource would have engaged in a sustained effort to make it clear that hardship customers were the sole customers affected and therefore they should look for a communication on this topic. Instead, only 156 out of 2,592 Connecticut customers enrolled in identity protection before the August 27, 2026, deadline. Response to OCC-73; Correspondence dated August 26, 2026, p. 15 (showing the August 27, 2026, deadline to enroll). That is a 6% response rate. Unsurprisingly, when every communication from Eversource downplayed what occurred, customers ignored the peril in which Eversource placed them.

[6] Response to OCC-81 states that "on May 20, 2026, Eversource received confirmation from IDX of the final list of impacted persons and their state of residence for purposes of notifications." If every customer was identified on May 20, it is unclear why Eversource waited another week to send the letter to affected customers unless Eversource was still determining the correct addresses after that date; at the same time, it is unclear how Eversource had identified the customers' "state of residence" without also determining their addresses.

V. Eversource mishandled this data breach.

A data breach is inherently a mistake, but companies can respond to mistakes in a way that demonstrates their managerial competence and their concern for their customers. Neither is evident in Eversource's actions. Eversource attempted to explain that this breach occurred only because the data was housed in the cloud and "Eversource would have detected the attack immediately if it had occurred on an Eversource-owned system because the Company's security tools would have generated internal notifications and/or blocked access to Company's files." Response to OCC-30. This leads to more questions than answers: why not deploy better protection for data in the cloud or why house customers' personal data in the cloud if Eversource knew it could not sufficiently protect the cloud data? A cybersecurity system does not inspire confidence when it relies on the bravado of the attacker to alert Eversource to the attack. Nor does a cybersecurity system inspire confidence when it fails to stop data from being downloaded once alerted to it, and when it continues to permit attacks (and breaches) for another week after being alerted to the attack.

Having realized that it leaked thousands of vulnerable Connecticut residents' personal information, OCC would have hoped Eversource would have taken numerous, high-profile steps to warn customers. This is the type of information to be shouted from the rooftops so that hardship customers know to either look for the IDX monitoring letter or proactively contact Eversource to enroll in the monitoring and protect themselves. Instead, Eversource spent the majority of its press release touting its supposed successes and emphasizing the customers who were not hurt rather than focusing on the customers who were. The date to enroll in monitoring then came and went, very few hardship customers enrolled, and a month later Eversource's CEO sat at a conference saying he was "very optimistic about [the] outcome" in the pending rate case and found comfort in PURA because "this commission right here is the one that took a Yankee Gas case that we got a draft decision that was $70 million, very low ROE. …By the time they got through with it, we got $104 million. We got the highest ROE in Connecticut, 9.47%," yet he never mentioned the cyberattack or the customers hurt by it. Docket No. 26-05-10, Response to OCC-944, Attachment 1, p. 11. It is not difficult to determine where Eversource's priorities lay: profit trumps protection of customer data.[7]

This report details multiple points at which Eversource failed its customers and significant portions of that failure can be attributed to Eversource's management. OCC reiterates its request that this investigation be incorporated into the existing rate case in Docket No. 26-05-10. In that rate case, the Authority is tasked with evaluating the very management that failed to proactively identify the cyberattack, exposed millions of files to the cyberattacker, and failed Eversource customers – the very management and cybersecurity for which Eversource is asking ratepayers to increase rates to fund. The rate case is the best vehicle in which to address systemic management and cybersecurity failures.[8]

---

[7] Joseph Nolan further stated he was pleased to report that "[Eversource] achieved 96% of [its storm] ask… $960 million in storm cost." Docket No. 26-05-10. Response to OCC-944, Attachment 1, p.3.

[8] Further, in its Responses to OCC-69 through OCC-71, Eversource left open the possibility of cost recovery for outside legal counsel, the trained expert to negotiate with the attacker, and IDX monitoring. In Docket No. 26-05-10, Eversource has proposed a performance incentive mechanism regarding the speed with which it enrolls hardship customers onto a discount rate following the date the customer provides Eversource qualifying proof of eligibility. .

OCC further recommends that, as a result of this incident, either in the Decision in this proceeding or as part of Docket No. 26-05-10, the Authority should order Eversource to have a third party audit its cybersecurity systems. The third party should examine this incident and all other aspects of Eversource's cybersecurity. Eversource's shareholders, not ratepayers, should bear the costs of this audit. Ratepayers have already borne the costs of this data release and should not also have to also pay for Eversource to fix issues that prudent management would have identified and solved without the need for a regulatory investigation.

OCC thanks the Authority for considering this Report.

Respectfully submitted,

STATE OF CONNECTICUT
OFFICE OF CONSUMER COUNSEL

CLAIRE E. COLEMAN
CONSUMER COUNSEL

By: /s/ Kimberly White
Kimberly White
Attorney
10 Franklin Square
New Britain, CT 06051
860.827.2695

CERTIFICATE OF SERVICE

I do hereby certify that on this day the foregoing document was filed with the Public Utilities Regulatory Authority, and copies thereof were served upon each person designated on the official service list in this proceeding in accordance with R.C.S.A. § 16-1-15.

Dated at New Britain, Connecticut this 13th day of November, 2026.

/s/Kimberly White
Commissioner of the Superior Court