follow industry guidelines for validating SS7 link diversity, which should be performed at a minimum of twice a year, and at least one of those validations should include a physical validation of equipment compared to the recorded documentation of diversity."[2] [redacted]. CenturyLink/Infinera created a "packet storm," equivalent to a Denial of Service ("DOS") attack against itself, that effected most or all of the nodes in the "Green" network, and for a several hours within the 37-hour window of the CenturyLink impairment, affected all "Green" network nodes utilized by the TSYS and TNS TDM circuits.

Further, the Emergency Communications Division ("ECD") of the Cybersecurity & Infrastructure Security Agency ("CISA") paraphrases physical diversity: "Communications resiliency means a network is able to withstand damages, thereby minimizing the likelihood of a service outage. Resiliency is the result of three key elements: route diversity, redundancy, and protective/restorative measures."[3] The additions of supplier and vendor diversity are not mentioned by CISA. TSYS believes that it had adequate physical diversity for the SS7 links (two geo-diverse data centers, connecting over two diverse circuits and using two physical cards toward TNS's similar configuration) but also believed that adding vendor diversity would have been better. [redacted]

UTC STAFF DATA REQUEST NO. 11:
Provide all documents, including but not limited to email, notes, diagrams, and any other documents that demonstrate any and all steps TSYS took to ensure that [redacted]

[2] The Communications Security, Reliability and Interoperability Council IV, Working Group 7, Final Report (2014), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC%20IV%20WG7%20Legacy%20Best%20Practices%20Final.pdf.

[3] Public Safety Communications Network Resiliency Self-Assessment Guidebook, Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Emergency Communications Division (2018), https://www.cisa.gov/sites/default/files/publications/DHS%20ECD%20Public%20Safety%20Communications%20Network%20Resiliency%20Self-Assessment%20Guidebook_11.29.18%20-%20FINAL.pdf.

RESPONSE: TSYS objects to this data request as overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. Without waiving these objections, TSYS provides the following response:

After the CenturyLink Outage in December 2018, [redacted]

[redacted]

UTC STAFF DATA REQUEST NO. 12:
Provide all documents, including but not limited to email, notes, diagrams, and any other documents that demonstrate any and all steps TSYS took to ensure that it utilized both [redacted]

RESPONSE:
TSYS objects to this data request as overly broad, unduly burdensome, calls for information that is irrelevant and disproportionate to the needs of this case, and is not reasonably calculated to lead to the discovery of admissible evidence. Without waiving these objections, TSYS provides the following response:

TSYS added [redacted] to further enhance the connection between ESInet 1 and ESInet 2. This mix of [redacted] was jointly discussed and designed by TSYS and TNS. TSYS conducted a good faith search for all documentation showing the steps TSYS took to ensure [redacted] can be seen in the test plan attached hereto as **Exhibit 3.b.**, which illustrates that [redacted]

REDACTED