Freight giant Estes refuses to deliver ransom, says personal data opened and stolen

By Jessica Lyons

Published: 2024-01-03 · Archived: 2026-04-05 18:51:25 UTC

One of America's biggest private freight shippers, Estes Express Lines, has told more than 20,000 customers that criminals stole their personal information.

"As you may be aware, on October 1, 2023, Estes discovered that an unauthorized threat actor had gained access to a portion of the company's IT network and deployed ransomware," it said in a letter mailed to 21,184 people [PDF]. "In accordance with the standard recommendation of the FBI and financial regulators, Estes did not pay the ransom."

The family-owned billion-dollar biz indeed disclosed the "cyberattack" in early October, and at the time said the intrusion affected its IT infrastructure. By October 24, chief operating officer Webb Estes posted a video on X announcing that the company had "completely restored our systems capabilities."

A month later, ransomware crew Lockbit took responsibility for the intrusion, and said it leaked data stolen from the biz on November 13.

Then, on New Year's Eve, Estes filed a data breach notification with the Maine Attorney General that provided some additional details about the digital break-in, which it now says was indeed ransomware.

The shipper says it's cooperating with the FBI, and a subsequent forensics investigation determined that the intruders stole personal information, although the sample notification letter doesn't specify which data the miscreants accessed. According to the Maine filing, it includes names or other personal identifier in combination with Social Security numbers, although the blank text in the letter indicates that the ransomware crew exfiltrated more than this.

Estes did not immediately respond to *The Register*'s questions about the intrusion, including what data the crooks stole, how they initially accessed the company's network, how much money they demanded, and why company exes made the decision to not pay the ransom.

This, of course, has become a hotly debated topic and it involves multiple factors ranging from the practical — does the victim organization have effective backups and how much money will downtime cost — to the more philosophical — will paying a ransom facilitate human trafficking and/or terrorism, or even just subsequent cybercrime?

Either choice can be extremely costly for victims. Caesars Entertainment reportedly paid a ransomware gang $15 million to decrypt its data and not leak its customers' info after a September intrusion, while fellow Las Vegas hotel and casino giant MGM Resorts said a similar attack cost it more than $100 million in losses after not paying up.

The US government advises organizations not to pay ransom demands, and some have called for a complete ban on extortion payments.

Estes says it's "not aware of any identity theft, fraud, or financial losses resulting from this incident."

It will also provide affected individuals with 12 months of free identity monitoring from Kroll. ®
