# Bond Case Briefs

*Municipal Finance Law Since 1971*

---

## Ransomware Attack on Hospital Shows New Risk for Muni-Bond Issuers.

- **The attack in part led to a breach of a covenant agreement**
- **The hospital spent $1 million in response to the attack**

Hackers have finally done what bond issuers may have feared most from cyber criminals.

A ransomware attack on Pleasant Valley Hospital in West Virginia was partly responsible for the hospital's breach of its covenant agreement, according to a notice to the hospital's bondholders from the trustee, WesBanco Bank. It appears to be the first time a cyber attack triggered a formal covenant violation, according to research firm Municipal Market Analytics.

The virus entered the hospital's system via emails sent 10 months before the cyber criminals asked the hospital for money, said Craig Gilliland, the hospital's chief financial officer. The information the criminals held for ransom did not contain patient data or confidential data, so it was "more of an annoyance," he added.

Because of the attack, the hospital was forced to spend about $1 million on new computer equipment and infrastructure improvements, Gilliland said. That cost, along with declining patient volume, caused the hospital's debt service coverage for the fiscal year that ended on Sept. 30 to fall to 78%, below the 120% the loan agreement requires, according to the material notice to bondholders.

Continue reading.

**Bloomberg**

By Mallika Mitra

February 5, 2020, 7:11 AM PST

Copyright © 2026 Bond Case Briefs | bondcasebriefs.com