UnitedHealth faces growing calls for accountability over cyberattack

- Tina Reed

, author of

Axios Vitals

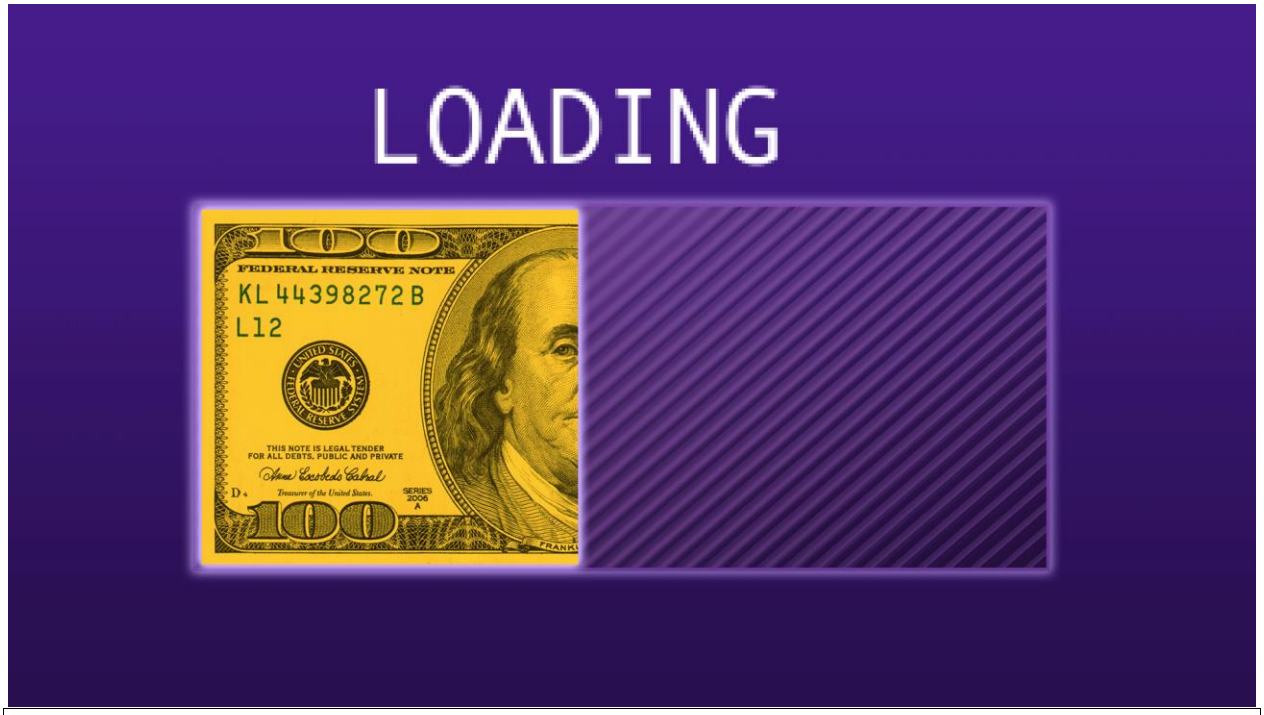

Illustration: Sarah Grillo/Axios

A central question that has emerged since a cyberattack on a UnitedHealth Group subsidiary is how the strike against a single company has wrought such chaos across an entire industry.

Why it matters: Hospitals, doctors' offices and pharmacies are still struggling with the fallout of the outage of Change Healthcare's payment system, as they worry emergency measureswon't be enough if the disruption drags on.

The big picture: Some cybersecurity experts point to UnitedHealth's buying spree, which among other things has allowed the nation's largest insurer to control a major piece of how medical claims are processed.

- Horizontal and vertical mergers that have become common among major U.S. companies, including in health care, create massive targets for cyber criminals, said Jason Hogg, executive-in-residence at Great Hill Partners and a former FBI special agent.
- "From a cybersecurity perspective, you can affect everything from patient records and hospitals to the actual payment system," Hogg said. "We have this massive exposure and it's a national security threat."

Others said there's too little oversight of the cybersecurity protecting such critical pieces of infrastructure — a situation they said is unimaginable in other sectors that depend on sensitive financial transactions.

- "Jamie Dimon would already be on Capitol Hill," if this had happened to JPMorgan Chase, said Boe Hartman, co-founder and chief technology officer of Nomi Health, who spent the majority of his career in the banking sector.
- "That's what stuns me. They've punched a hole in 20% of the U.S. economy ... and it appears at the moment no one's being held to account," Hartman said.

The intrigue: Federal technical standards governing electronic data exchange may actually have made this attack more damaging, argues a nonprofit that supports tougher antitrust enforcement.

- These health department guidelines, known as electronic data interchange standards, may have helped concentrate the use of Change Healthcare's systems as a clearinghouse for payments by making it difficult for providers to use more than one clearinghouse at a time, according to the American Economic Liberties Project.
- That's kind of like making it difficult to use both Visa and Mastercard, said Benjamin Jolley, a senior fellow with the group and a pharmacist directly affected by the outages, said during a press call Tuesday evening.

- "Apparently everyone decided that using the 800-pound gorilla company would mean that you didn't have problems," Jolley said, referring to UnitedHealth, which acquired Change Healthcare in 2022.
- The Department of Health and Human Services did not respond to a request for comment Tuesday evening.

What we're watching: The pressure is mounting on UnitedHealth, which has offered loans to affected providers.

- Biden administration officials on Tuesday pushed UnitedHealth executives, including CEO Andrew Witty, to do more to stabilize providers during a meeting with health care groups, according to a readout from HHS.
- "We urge UnitedHealth Group to take responsibility to ensure no provider is compromised by their cash flow challenges stemming from this cyberattack," HHS Secretary Xavier Becerra and acting Labor Secretary Julie Su wrote over the weekend.

UnitedHealth Group did not respond to specific questions from Axios on Tuesday