Opening Remarks
Chair Cathy McMorris Rodgers
Subcommittee on Oversight and Investigations
Hearing, "Examining the Change Healthcare Cyberattack"
May 1, 2024

OPENING

Thank you, Mr. Witty, for agreeing to testify before us today.

Like Chair Griffith, I was disappointed your organization declined our original invitation to testify on the cyberattack on Change Healthcare—one of your subsidiary companies—before our health subcommittee but appreciate your cooperation in being here today.

Most Americans have likely never heard of Change Healthcare, despite how crucial its functioning is to ensuring their access to care.

Change acts as a clearing house for 15 billion medical claims each year—that means more than roughly 50 percent of all claims pass through Change.

15 billion patient interactions with the health care system.

That covers everything from routine checkups with primary care physicians to lifesaving cancer treatments with specialists.

Things we, until recent weeks, probably took for granted.
In 2022, your company acquired Change Healthcare as part of a growing creep into every corner of our health care system.

Under the United Health Group umbrella, resides:

- An insurance company with more than 40 million covered lives across Medicare, Medicaid, and commercial markets
- A PBM, that managed 159 billion dollars in drug spending last year
- A provider group that owns roughly one in every twelve doctors in the United States
- A bank, that makes payday loans to providers

To name just a few of the ventures under your purview...

I say this to emphasize the massive responsibility that comes with your position, Mr. Witty...

When a family of four... that is being crushed by inflation... forks over more than twenty thousand dollars per year for their health insurance...

When a senior citizen sees the AARP brand on your Medicare product...

When the taxpayer funnels tens of billions in subsidies to your company...

There is a reasonable expectation that they will get a baseline level of value for their hard-earned money.

But I'll set the bar higher: You have a responsibility to protect the data of the people who have put their trust in you.

And I'll put it bluntly: **In this case, you failed.**

THE CYBERATTACK

On February 21 of this year, Change Healthcare announced it was hit with a cyberattack, severely disrupting the health care ecosystem for providers, payers, and patients.

It has been more than two months since this cyberattack, and, according to your company's own website, Change has yet to fully restore its services...

... And many negative impacts for the health care system persist.

As your written testimony lays out, criminal hackers gained access to Change Healthcare through "compromised credentials"...

...remotely accessing the company's portal nine days before your company publicly announced the ransomware attack.

This portal did not have multi-factor authentication enabled—a relatively basic protection against cyberattacks—which allowed the cyber criminals to unlock the door and break into your systems.

Multi-factor authentication would be a basic expectation for a company handling the breadth of sensitive information that Change Healthcare does.

FALLOUT – RANSOM

It has now been reported your company paid a ransom to the cyber criminals.

While I have grave concerns with the precedent you created by rewarding the criminals...

...I understand that it would be a difficult decision to weigh that against protecting Americans' data.

But here's the problem: **It did not stop the data leak.**

Americans personal and private health information is on the dark web.

This is private health data you were responsible for protecting.

Mr. Witty, I suspect that decision will be a case study in crisis mis-management for decades to come.

FALLOUT - PROVIDERS

I would be remiss if I didn't note that providers—especially smaller providers and solo practitioners—continue to provide uncompensated care as submitted claims cannot be processed through payers.

It's been reported that some providers have contemplated closing, and others have been forced to rely on volunteers to care for patients.

Others have had to furlough staff so their employees can apply for unemployment benefits.

I look forward to hearing how this is going to be fixed as soon as possible.

CLOSING

I'll note in closing that we're here today to learn more about what happened in the lead up and during the attack, and what you, Mr. Witty, are doing to fix it and prevent it from happening again.

The American people—particularly the millions who rely upon Change's services and those whose information was leaked—deserve answers.

I yield back.