RUBEN GALLEGO
3RD DISTRICT, ARIZONA
COMMITTEES:
ARMED SERVICES
SUBCOMMITTEES:
RANKING MEMBER, INTELLIGENCE AND SPECIAL OPERATIONS
TACTICAL AIR AND LAND FORCES
NATURAL RESOURCES
SUBCOMMITTEES:
INDIAN AND INSULAR AFFAIRS
WATER, WILDLIFE, AND FISHERIES
OVERSIGHT AND INVESTIGATIONS

Congress of the United States
House of Representatives
Washington, DC 20515–0307

DC OFFICE:
1114 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4065

DISTRICT OFFICE:
1601 N 7TH STREET
SUITE 310
PHOENIX, AZ 85006-2481
(602) 256-0551

March 5, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
245 Murray Lane
Washington, DC 20528

The Honorable Xavier Becerra
Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Director Easterly and Secretary Becerra:

I am writing regarding the recent cyber-attack on Change Healthcare, a unit of UnitedHealth Group and Optum, and related difficulties faced by pharmacies, providers, hospitals, and patients across my home state of Arizona.

Pharmacies and providers across the country, including in Arizona, have been unable to process patient insurance, forcing patients to choose between forgoing critical medications or paying out of pocket with the hopes of receiving reimbursement. I am deeply concerned that the negative impacts on Arizona's health infrastructure and access to care for Arizonans may become irreversible, and I request you use all available resources and authorities to provide relief.

As you know, Change Healthcare, which processes prescriptions to insurance for pharmacies, first reported a potential incident at 2:15 am EST on Wednesday, February 21st. Initially described as an "enterprise-wide connectivity issue," UnitedHealth later noted in its required Security and Exchange Commission (SEC) cyber security disclosure that the ongoing event involves, "A suspected nation-state associated cyber security threat actor," who had, "gained access to some of the Change Healthcare information technology systems." However, it now appears that the cyber-attack may have originated from an unaffiliated ransomware gang, contradicting UnitedHealth's initial filing.

In a statement, Change Healthcare says that it disconnected its systems to prevent further impact once it became aware of the outside threat. The shutdown also impacted hospitals and providers who have been unable to bill insurers or have not had the resources needed to purchase equipment, treatments, and supplies.

It appears that this attack is related to a vulnerability discovered in the ScreenConnect app from ConnectWise, which is used for remote access for services such as IT support. Once ConnectWise discovered the vulnerability, it released a security fix on Monday, February 19th –

two days prior to the first bulletin of a cyber security incident from Change Healthcare. While it is not publicly known if Change Healthcare attempted to implement the security fix, the two-day window between the public disclosure of the vulnerability, rated as critical when first reported by ConnectWise, and when that vulnerability was exploited is extremely concerning.

As of the writing of this letter, Change Healthcare's systems remain disconnected. While it is unclear still unclear the full impacts of this breach, UnitedHealth's Optum, which uses Change Healthcare for prescription processing, supplies technology services for more than 67,000 pharmacies and care to over 125,000,000 individual customers.

I have heard firsthand the impacts of this shutdown on Arizona's health care community, including pharmacies, providers, hospitals, and patients. Pharmacies, for example, have been unable to offer cost-sharing to patients. This has forced patients to pay full price for medications at the point of sale and then file directly with the insurance company for reimbursement, a confusing and time-consuming process for families, seniors, and Arizonans with disabilities.

Hospitals and providers are also hurting, and some offices may be forced to close permanently. Private providers and health care systems already face significant operational overhead, and the loss of revenue and administrative burden faced by business owners who are operating at slim margins are not sustainable. As we enter the second week of this shutdown, I fear that the situation may become even more dire as patients who cannot go to their normal providers are forced to go to emergency rooms, and as specialists and surgical centers are unable to restock on lifesaving, high-cost medications and supplies.

I request that you immediately use all available resources and authorities at your disposal to help Arizona's health care sector and patients who may be forced to close permanently if this situation is not resolved. That includes administrative support for impacted entities, a coordinated cyber security response to resume operations across the country, assistance for Arizona's health care sector, and guidance for impacted patients.

Additionally, I request answers to the following questions:

1. When was CISA first informed of the vulnerability in the ScreenConnect application?

2. To the best of your knowledge, was this vulnerability communicated to UnitedHealth or Optum, or did UnitedHealth request technical assistance to respond to the vulnerability?

3. When were both CISA and HHS made aware of both breaches of Change Healthcare's systems? Was this before or after the system shutdown?

4. What support has been offered to impacted entities, including providers, pharmacies, and hospital systems? Has any guidance been made available or distributed? Have any resources or administrative support been offered to alleviate the burden on the health care sector?

Thank you in advance for your attention to this matter.

Sincerely,

Ruben Gallego
MEMBER OF CONGRESS