Crapo Statement at Hearing on Change Healthcare Cyberattack
May 1, 2024

Washington, D.C.--U.S. Senate Finance Committee Ranking Member Mike Crapo (R-Idaho) delivered the following remarks at a hearing entitled "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next."

As prepared for delivery:

"Thank you, Mr. Chairman, and thank you Mr. Witty for being here today.

"On February 21, 2024, UnitedHealth Group learned that its subsidiary, Change Healthcare, was likely the victim of a cyberattack launched by 'a suspected nation-state associated cyber security threat actor.'

"In response, Change, the nation's largest health care clearinghouse—which processes $1.5 trillion in medical claims annually—disconnected all of its systems to prevent the hackers from obtaining additional data.

"The fallout from this unprecedented attack has affected the entire health care sector. By crippling Change's functionality, the hackers left providers unable to verify patients' insurance coverage, submit claims and receive payments, exchange clinical records, generate cost estimates and bills, or process prior authorization requests.

"In the immediate aftermath of the attack, many providers had to rely on reserves to cover the resulting revenue losses. An American Hospital Association survey found that more than 90 percent of hospitals were financially impacted by the cyberattack, with more than 70 percent reporting that the outage had directly affected their ability to care for patients.

"More than two weeks after the cyberattack was announced, the Department of Health and Human Services released a public statement and guidance related to the incident. On March 9, the Centers for Medicare and Medicaid Services made accelerated and advance payments available to impacted Medicare providers.

"The Administration's delay exacerbated an already uncertain landscape, leaving providers and patients with reasonable concerns about access to essential medical services and life-saving drugs.

"While the February hack on Change was by far the most disruptive cyberattack on the health care industry to date, it was certainly not the first. According to a report by the Federal Bureau of Investigation, the health care sector experienced more ransomware attacks than any other critical infrastructure sector in 2023.

“In addition to the processing and revenue issues experienced by providers, patients’ private identification and health care information was obtained by malicious actors during the breach.

“Unfortunately, personal health care data has become increasingly attractive to cyber criminals, who seek to use that information for blackmail or identity theft. For patients, the emotional and financial effects of leaked private information can have a devastating impact for years.

“Although many of Change’s functions have now resumed, trust in the security of its platforms needs to be rebuilt.

“We owe it to American patients and to our frontline health care providers, from health systems to clinicians and community pharmacies, to ensure that this does not, and cannot, happen again.

“Today’s hearing offers a valuable opportunity to learn from United’s experience so we can better protect against, and quickly react to, future cyberattacks.

“Gaining a deeper understanding of how the hackers infiltrated Change will help identify and address gaps in our existing cybersecurity infrastructure.

“Evaluating steps taken by United in response to the attack, from disconnecting its platforms to notifying law enforcement, will offer lessons on how to build a more resilient and collaborative health care system moving forward.

“We must also assess the response of the federal government, which plays a critical role in these efforts. HHS has a responsibility to serve as a central hub for coordination, convening insights from other branches of government and the private sector to deploy timely information about active threats, as well as best practices to deter intrusions and resources should an attack occur.

“Thank you, Mr. Witty, for being here to discuss building a more secure, resilient and responsive health care system.

“Thank you, Mr. Chairman.”