

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

October 15, 2024

Andrew Witty
Chief Executive Officer
UnitedHealth Group
P.O. Box 1459
Minneapolis, MN 55440-1459

Dear Mr. Witty:

I write to seek answers to questions for the record following your testimony before the Senate Finance Committee (“the Committee”) in June 2024 that to date have not been satisfactorily answered.

UnitedHealth Group’s (“UHG”) subsidiary Change Healthcare experienced a major ransomware incident in February 2024 (“the ransomware incident”) that resulted in the theft of most Americans’ private health information, seriously impacted patient care, and triggered a major financial shock wave that harmed hospitals, doctors, and other providers. You testified about this incident before the Committee in June, during which you provided vague, unclear information about the incident and the degree to which it was caused by your company’s lax cybersecurity practices. I sent written follow-up questions after the hearing. Your responses did not satisfactorily answer my questions. My staff have also asked several times for answers to these questions. Your staff have responded, but again, without satisfactorily answering the questions.

Congress has a responsibility to conduct rigorous oversight to determine what legislative actions might be necessary in the wake of the most significant cyberattack against the U.S. health care sector to date. To that end, please provide the Committee with full answers to these questions, no later than November 8, 2024:

1. You testified before the Committee that the first server that was compromised was not protected with multi-factor authentication, a basic cybersecurity best practice. In response to post-hearing written questions and follow-up emails from my staff, UHG confirmed that the company regularly hired auditors who review the security of the company’s technology infrastructure. Prior to February 2024, had auditors reviewed the security of the server that was first compromised?
2. In response to post-hearing questions for the record, you acknowledged that during the ransomware incident, after gaining their initial foothold in Change Healthcare’s network,

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

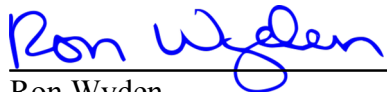
malicious actors gained privileged access to one of the crown jewels of a corporate IT network, the Microsoft Active Directory Server. What specific technical technique did the malicious actors utilize to escalate privilege? Prior to February 2024, had auditors identified this privilege escalation technique and recommended Change Healthcare implement defenses against it?

3. What specific defensive steps have you taken to ensure that the privilege escalation technique used against Change Healthcare's Active Directory server has been neutralized company-wide, and cannot be exploited by hackers who gain access to your company's systems in the future? How have you determined that these defenses are effective against the techniques used in the Change Healthcare ransomware incident?

Please also provide copies of all external cybersecurity audit reports of Change Healthcare's technology infrastructure, for the five years preceding the ransomware incident, including those that took place before UHG's purchase of Change Healthcare in 2022. Please identify the names of the companies that performed the audits, but you may, as appropriate, redact the names of the auditors' employees that appear in the reports.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator
Chairman, Committee on
Finance